

VMware Cloud Director 설치, 구성 및 업그레이드 가이드

수정 날짜: 2021년 4월 8일
VMware Cloud Director 10.2

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware 코리아
서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

Copyright © 2010-2021 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

목차

VMware Cloud Director™ 설치, 구성 및 업그레이드 가이드 7

1 VMware Cloud Director 아키텍처 8

2 VMware Cloud Director 하드웨어 및 소프트웨어 요구 사항 11

VMware Cloud Director에 대한 네트워크 구성 요구 사항 12

네트워크 보안 요구 사항 13

3 VMware Cloud Director 장치의 배포, 업그레이드 및 관리 15

장치 배포 및 데이터베이스 고가용성 구성 15

VMware Cloud Director 장치의 자동 페일오버 18

실패한 기본 셀의 자동 펜싱 20

VMware Cloud Director 장치 배포 준비 20

VMware Cloud Director 장치를 위한 전송 서버 스토리지 준비 21

VMware Cloud Director용 NSX Data Center for vSphere 설치 및 구성 22

VMware Cloud Director용 NSX-T Data Center 설치 및 구성 23

VMware Cloud Director 장치의 배포 및 초기 구성 25

VMware Cloud Director 장치 크기 조정 지침 26

VMware Cloud Director 장치 배포를 위한 사전 요구 사항 31

vSphere Client를 사용하여 VMware Cloud Director 장치 배포 31

VMware OVF Tool을 사용하여 VMware Cloud Director 장치 배포 38

HTTPS 및 콘솔 프록시 통신을 위해 서명된 와일드카드 인증서를 사용하여 VMware Cloud Director 장치 배포 46

CA 서명된 SSL 인증서를 생성하고 VMware Cloud Director 장치로 가져오기 48

개인 키 및 CA 서명된 SSL 인증서를 VMware Cloud Director 장치로 가져오기 51

VMware Cloud Director 장치 배포 후 작업 53

VMware Cloud Director 장치 루트 암호 변경 58

VMware Cloud Director 장치 업그레이드 및 마이그레이션 59

업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드 62

VMware Update Repository를 사용하여 VMware Cloud Director 장치 업그레이드 65

업그레이드 실패 시 VMware Cloud Director 장치 롤백 67

외부 PostgreSQL 데이터베이스를 사용하는 VMware Cloud Director를 VMware Cloud Director 장치에 마이그레이션 68

VMware Cloud Director 업그레이드 후 작업 73

연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager 업그레이드 73

vCenter Server 시스템, ESXi 호스트 및 NSX Edge 업그레이드 74

VMware Cloud Director 장치 관리 76

VMware Cloud Director 장치의 내장된 데이터베이스 백업 및 복원	76
VMware Cloud Director 장치의 페일오버 모드 변경	83
VMware Cloud Director 데이터베이스에 대한 외부 액세스 구성	83
VMware Cloud Director 장치에 대한 SSH 액세스 활성화 또는 비활성화	84
VMware Cloud Director 장치에서 FIPS 모드 활성화 또는 비활성화	85
VMware Cloud Director 장치 SNMP 에이전트 구성	87
VMware Cloud Director 장치의 DNS 설정 편집	94
VMware Cloud Director 장치 네트워크 인터페이스에 대한 정적 경로 편집	94
VMware Cloud Director 장치의 구성 스크립트	96
VMware Cloud Director 장치 인증서 갱신	96
자체 서명된 내장형 PostgreSQL 및 VMware Cloud Director 장치 관리 UI 인증서 교체	98
VMware Cloud Director 장치를 위한 전송 서버 스토리지 바꾸기	98
VMware Cloud Director 장치에서 내장형 PostgreSQL 데이터베이스의 용량 늘리기	100
VMware Cloud Director 장치에서 PostgreSQL 구성 수정	101
데이터베이스 고가용성 클러스터에서 실행 중인 대기 셀 등록 취소	102
데이터베이스 고가용성 클러스터에서 기본 및 대기 셀의 역할 전환	102
MQTT 클라이언트를 사용하여 이벤트, 작업 및 메트릭 구독	104
자동 스케일 그룹	105
VMware Cloud Director 장치 데이터베이스 클러스터 상태 모니터링	107
VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기	107
VMware Cloud Director 장치 서비스 상태 보기	109
데이터베이스 고가용성 클러스터에서 연결 상태 확인	109
데이터베이스 고가용성 클러스터에서 노드의 복제 상태 확인	110
VMware Cloud Director 서비스 상태 확인	112
VMware Cloud Director 장치 데이터베이스 클러스터 복구	112
고가용성 클러스터에서 기본 셀 장애로부터 복구	113
고가용성 클러스터에서 대기 셀 장애로부터 복구	115
데이터베이스 고가용성 클러스터에서 실패한 기본 또는 대기 셀 등록 취소	116
장치 문제 해결	117
VMware Cloud Director 장치의 로그 파일 검토	117
장치 배포 후 VMware Cloud Director 셀이 시작되지 않음	118
초기 장치 구성 중에 NFS 검증 후 복구에 실패함	118
VMware Cloud Director 장치에 마이그레이션하거나 복원할 때 VMware Cloud Director 서비스를 재구성하지 못함	122
VMware Cloud Director 장치 대기 노드에 연결할 수 없는 상태가 됨	122
VMware Cloud Director 장치 대기 노드가 연결되지 않은 상태가 됨	125
클러스터 상태가 SSH 문제를 나타냄	127
로그 파일을 사용하여 VMware Cloud Director 업데이트 및 패치 문제 해결	131
VMware Cloud Director 업데이트 확인 실패	131
VMware Cloud Director의 최신 업데이트 설치 실패	132

4 Linux에서 VMware Cloud Director 설치, 업그레이드 및 관리 133

구성 계획 133

VMware Cloud Director 설치 준비 134

Linux에서 VMware Cloud Director용 외부 PostgreSQL 데이터베이스 구성 134

Linux에서 VMware Cloud Director를 위한 전송 서버 스토리지 준비 136

VMware 공용 키 다운로드 및 설치 137

VMware Cloud Director용 NSX Data Center for vSphere 설치 및 구성 138

VMware Cloud Director용 NSX-T Data Center 설치 및 구성 139

Linux에 VMware Cloud Director 설치 140

서버 그룹의 첫 번째 구성원에 VMware Cloud Director 설치 142

Linux에 VMware Cloud Director에 대한 SSL 인증서 생성 및 관리 143

네트워크 및 데이터베이스 연결 구성 150

서버 그룹의 추가 구성원에 VMware Cloud Director 설치 157

VMware Cloud Director 설치 후 작업 159

Linux용 VMware Cloud Director에 대한 공개 주소 사용자 지정 159

기간별 메트릭 데이터 저장을 위한 Cassandra 데이터베이스 설치 및 구성 160

외부 PostgreSQL 데이터베이스에서 추가 구성 수행 162

RabbitMQ AMQP 브로커 설치 및 구성 163

MQTT 클라이언트를 사용하여 이벤트, 작업 및 메트릭 구독 164

자동 스케일 그룹 165

Linux에서 VMware Cloud Director 업그레이드 167

VMware Cloud Director 설치의 오케스트레이션된 업그레이드를 수행 170

수동으로 VMware Cloud Director 설치를 업그레이드 172

데이터베이스 업그레이드 유틸리티 참조 177

VMware Cloud Director 업그레이드 후 작업 179

연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager 업그레이드 180

vCenter Server 시스템, ESXi 호스트 및 NSX Edge 업그레이드 180

5 셀 관리 도구 참조 사항 183

VMware Cloud Director 설치 구성 186

레거시 API 끝점에 대한 서비스 제공자 액세스 비활성화 188

셀 관리 189

셀 애플리케이션 관리 191

데이터베이스 연결 속성 업데이트 192

손상된 스케줄러 데이터 검색 및 복구 195

HTTPS 및 콘솔 프록시 끝점에 대한 자체 서명된 인증서 생성 196

HTTPS 및 콘솔 프록시 끝점에 대한 인증서 바꾸기 198

외부 서비스에서 SSL 인증서 가져오기 199

vSphere 리소스에서 끝점 인증서 가져오기 200

테스트 연결 거부 목록 구성	201
모든 활성 셀의 FIPS 상태 보기	202
허용되는 SSL 암호화 목록 관리	203
허용되는 SSL 프로토콜 목록 관리	206
메트릭 수집 및 게시 구성	208
Cassandra 메트릭 데이터베이스 구성	211
시스템 관리자 암호 복구	212
작업의 실패 상태 업데이트	213
감사 메시지 처리 구성	214
e-메일 템플릿 구성	216
연결이 끊어진 VM 찾기	219
VMware 고객 환경 향상 프로그램 참여 또는 탈퇴	221
애플리케이션 구성 설정 업데이트	222
카탈로그 동기화 임계치 조절 구성	222
VMware Cloud Director 사용자 인터페이스에 대한 액세스 실패 문제 해결	223
vCenter VM 검색 디버깅	224
다중 사이트에 스트레치된 네트워크에 대한 MAC 주소 재생성	226
VMware Cloud Director 셀의 데이터베이스 IP 주소 업데이트	227

6 VMware Cloud Director 로그 수집 230

7 VMware Cloud Director 소프트웨어 제거 232

VMware Cloud Director™ 설치, 구성 및 업그레이드 가이드

"VMware Cloud Director 설치, 구성 및 업그레이드 가이드"는 VMware Cloud Director™ 소프트웨어를 설치 및 업그레이드하고 VMware vSphere®, VMware NSX® for vSphere® 및 VMware NSX-T™ Data Center와 작동하도록 구성하는 방법에 대한 정보를 제공합니다.

대상 사용자

"VMware Cloud Director 설치, 구성 및 업그레이드 가이드"는 VMware Cloud Director 소프트웨어를 설치 또는 업그레이드하려는 모든 사용자를 대상으로 합니다. 이 문서의 정보는 Linux, Windows, IP 네트워크 및 vSphere에 대해 잘 알고 있는 숙련된 시스템 관리자로 작성되었습니다.

VMware Cloud Director 아키텍처

1

VMware Cloud Director 서버 그룹은 Linux 또는 VMware Cloud Director 장치의 배포에 설치된 하나 이상의 VMware Cloud Director 서버로 구성됩니다. 그룹 내의 각 서버는 VMware Cloud Director 셀이라고 하는 서비스 컬렉션을 실행합니다. 모든 셀은 단일 VMware Cloud Director 데이터베이스 및 전송 서버 스토리지를 공유하고 vSphere 및 네트워크 리소스에 연결됩니다.

중요 하나의 서버 그룹에서 Linux에 설치된 VMware Cloud Director 및 VMware Cloud Director 장치 배포의 혼합은 지원되지 않습니다.

VMware Cloud Director 고가용성 보장하려면 서버 그룹에 두 개 이상의 VMware Cloud Director 셀을 설치해야 합니다. 타사 로드 밸런서를 사용할 때 다운타임 없는 자동 페일오버를 보장할 수 있습니다.

VMware Cloud Director 설치를 여러 VMware vCenter Server[®] 시스템 및 이 시스템이 관리하는 VMware ESXi[™] 호스트에 연결할 수 있습니다. 네트워크 서비스의 경우 VMware Cloud Director가 vCenter Server와 연결된 NSX Data Center for vSphere를 사용하거나 VMware Cloud Director에 NSX-T Data Center를 등록할 수 있습니다. 혼합된 NSX Data Center for vSphere 및 NSX-T Data Center도 지원됩니다.

그림 1-1. VMware Cloud Director Linux 설치 아키텍처 다이어그램

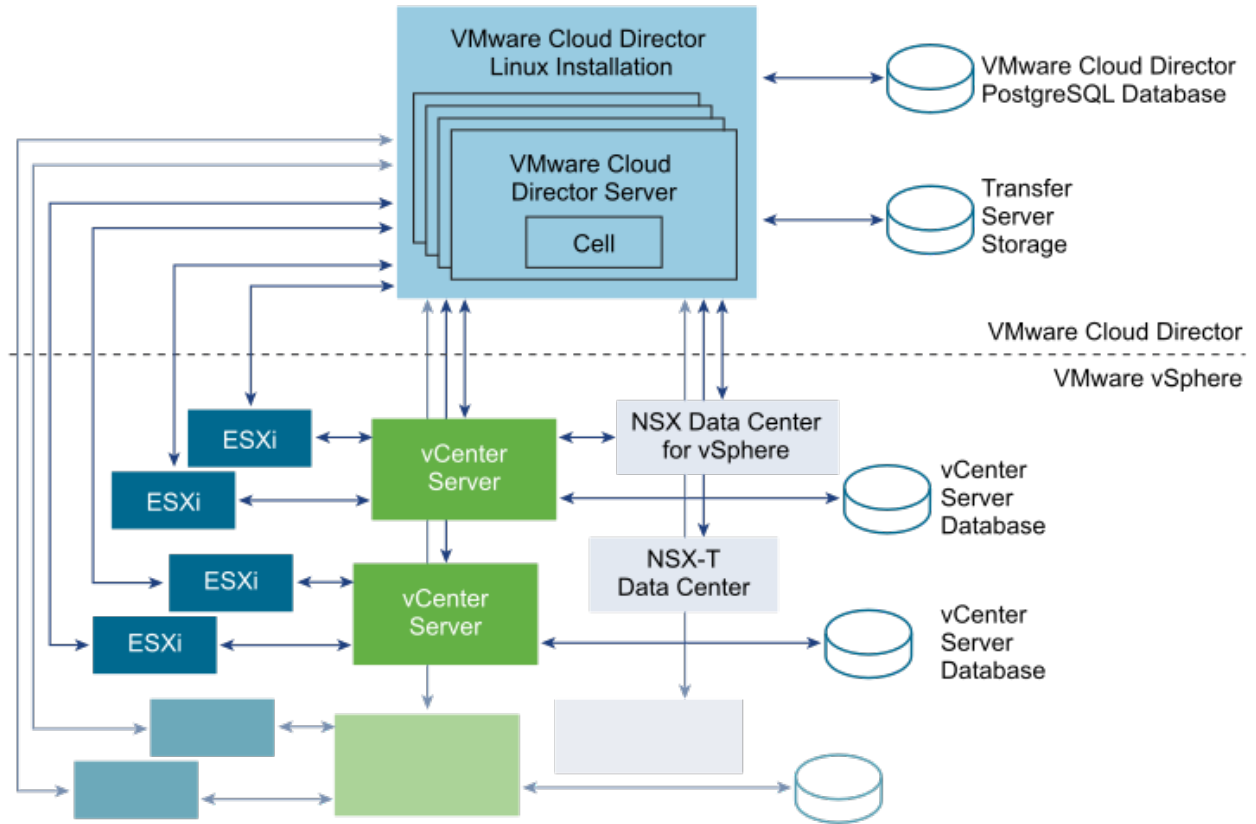
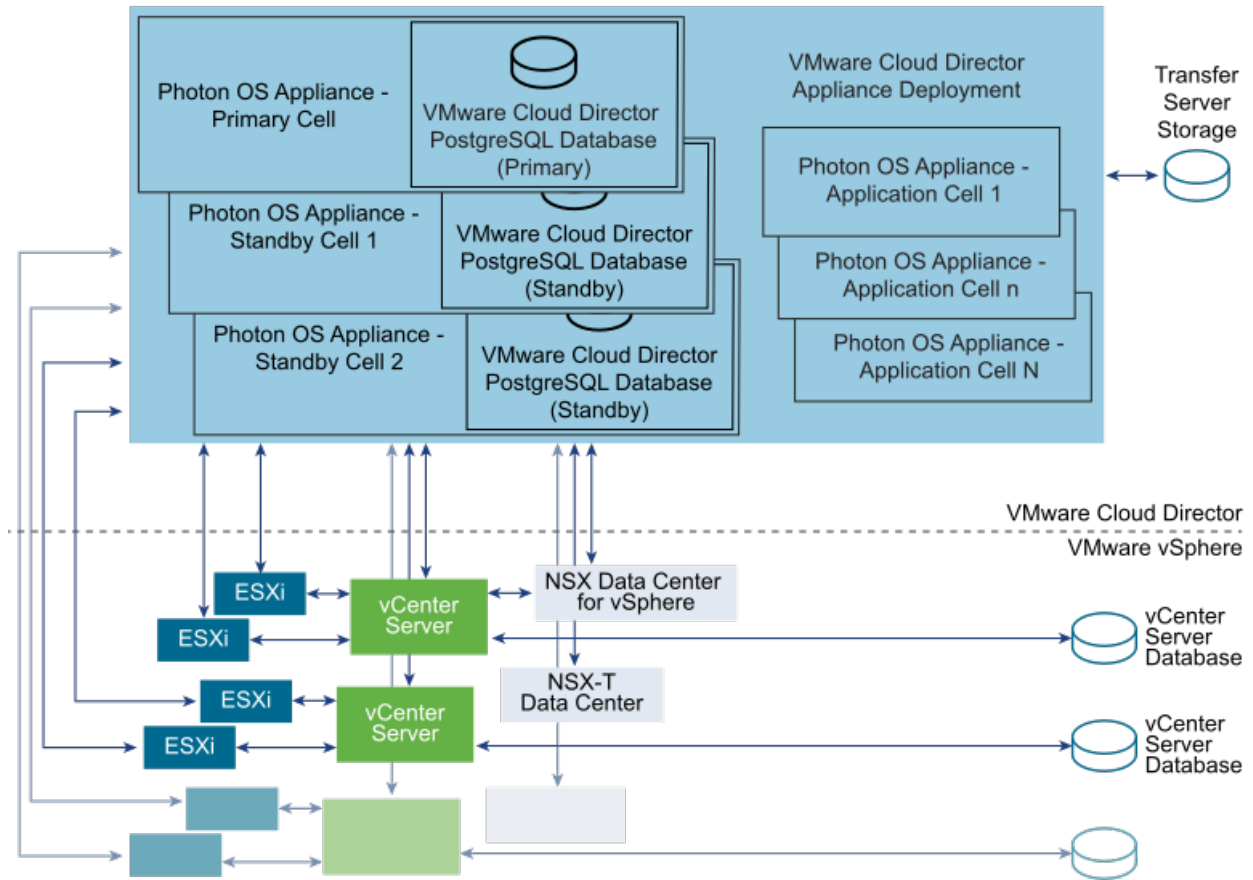


그림 1-2. VMware Cloud Director 장치 아키텍처 다이어그램



Linux에 설치된 VMware Cloud Director 서버 그룹은 외부 데이터베이스를 사용합니다.

장치 배포로 구성된 VMware Cloud Director 서버 그룹은 서버 그룹 첫 번째 구성원의 내장형 데이터베이스를 사용합니다. 장치의 인스턴스 2개를 동일한 서버 그룹의 대기 셀로 배포하여 VMware Cloud Director 데이터베이스 고가용성을 구성할 수 있습니다. 장치 배포 및 데이터베이스 고가용성 구성의 내용을 참조하십시오.

그림 1-3. 내장형 데이터베이스 고가용성 클러스터를 구성하는 VMware Cloud Director 장치

VMware Cloud Director 설치 및 구성 프로세스는 셀을 생성하여 공유 데이터베이스 및 전송 서버 스토리지에 연결하고 **시스템 관리자** 계정을 생성합니다. 그런 다음 **시스템 관리자**가 vCenter Server 시스템, ESXi 호스트 및 NSX Manager 또는 NSX-T Manager 인스턴스에 대한 연결을 설정합니다.

vSphere 및 네트워크 리소스를 추가하는 방법에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"의 내용을 참조하십시오.

VMware Cloud Director 하드웨어 및 소프트웨어 요구 사항

2

VMware Cloud Director 서버 그룹에 속해 있는 각 서버는 특정 하드웨어 및 소프트웨어 요구 사항을 충족해야 합니다. 또한 지원되는 데이터베이스는 그룹의 모든 구성원이 액세스할 수 있어야 합니다. 각 서버 그룹에는 vCenter Server 시스템, NSX Manager 인스턴스 및 하나 이상의 ESXi 호스트에 대한 액세스 권한이 필요합니다.

다른 VMware 제품과의 호환성

VMware Cloud Director 및 기타 VMware 제품 간 호환성에 대한 최신 정보는 "VMware 제품 상호 운용성 매트릭스" (http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php)를 참조하십시오.

vSphere 구성 요구 사항

VMware Cloud Director와 함께 사용하려는 vCenter Server 인스턴스 및 ESXi 호스트는 특정 구성 요구 사항을 충족해야 합니다.

- VMware Cloud Director 외부 네트워크 또는 네트워크 풀로 사용하려는 vCenter Server 네트워크는 VMware Cloud Director에서 사용할 임의의 클러스터에 있는 모든 호스트에서 사용할 수 있어야 합니다. 데이터 센터의 모든 호스트가 이러한 네트워크를 사용할 수 있도록 하면 VMware Cloud Director에 새 vCenter Server 인스턴스를 추가하는 작업이 간소화됩니다.
- NSX Data Center for vSphere에서 지원되는 격리된 네트워크 및 네트워크 풀에는 vSphere Distributed Switch가 필요합니다.
- VMware Cloud Director와 함께 사용되는 vCenter Server 클러스터는 vSphere DRS 자동화 수준을 **완전히 자동화됨**으로 지정해야 합니다. Storage DRS는 모든 자동화 수준으로 구성할 수 있습니다(사용되도록 설정된 경우).
- vCenter Server 인스턴스는 해당 호스트를 신뢰해야 합니다. VMware Cloud Director에서 관리되는 모든 클러스터의 모든 호스트는 확인된 호스트 인증서를 요구하도록 구성되어야 합니다. 특히 모든 호스트에 대해 일치하는 지문을 결정하고 비교하고 선택해야 합니다. "vCenter Server 및 호스트 관리" 설명서에서 SSL설정 구성을 참조하십시오.

지원되는 플랫폼, 데이터베이스 및 브라우저

이 VMware Cloud Director 릴리스에서 지원하는 서버 플랫폼, 브라우저, LDAP 서버 및 데이터베이스에 대한 자세한 내용은 "VMware Cloud Director 릴리스 정보"를 참조하십시오.

디스크 공간, 메모리 및 CPU 요구 사항

디스크 공간, 메모리 및 CPU 요구 사항에 대한 자세한 내용은 [VMware Cloud Director 장치 크기 조정 지침](#) 항목을 참조하십시오.

공유 스토리지

VMware Cloud Director 전송 서비스용 NFS 또는 기타 공유 스토리지 볼륨입니다. 스토리지 볼륨은 확장이 가능하고 서버 그룹에 속한 모든 서버에서 액세스할 수 있어야 합니다.

본 장은 다음 항목을 포함합니다.

- [VMware Cloud Director에 대한 네트워크 구성 요구 사항](#)
- [네트워크 보안 요구 사항](#)

VMware Cloud Director에 대한 네트워크 구성 요구 사항

VMware Cloud Director의 안전하고 안정적인 작동은 호스트 이름, 네트워크 시간 서비스 및 기타 서비스에 대한 정방향 및 역방향 조회를 지원하는 안전하고 안정적인 네트워크에 달려 있습니다. VMware Cloud Director를 설치하기 전에 네트워크가 다음과 같은 요구 사항을 충족해야 합니다.

VMware Cloud Director 서버, 데이터베이스 서버, vCenter Server 시스템 및 NSX 구성 요소를 연결하는 네트워크는 몇 가지 요구 사항을 충족해야 합니다.

IP 주소

각 VMware Cloud Director 서버는 두 개의 서로 다른 SSL 끝점을 지원해야 합니다. 한 끝점은 HTTPS 서비스용이고, 다른 끝점은 콘솔 프록시 서비스용입니다. 이러한 끝점은 별도의 IP 주소이거나 두 개의 서로 다른 포트를 사용하는 단일 IP 주소일 수 있습니다. IP 별칭 또는 여러 개의 네트워크 인터페이스를 사용하여 이러한 주소를 생성할 수 있습니다. Linux `ip addr add` 명령을 사용하여 두 번째 주소를 생성하지 마십시오.

VMware Cloud Director 장치는 콘솔 프록시 서비스에 대해 사용자 지정 포트가 8443인 자체 `eth0` IP 주소를 사용합니다.

콘솔 프록시 주소

콘솔 프록시 끝점으로 구성된 IP 주소는 SSL 종료 로드 밸런서 또는 역방향 프록시 뒤에 위치해서는 안 됩니다. 모든 콘솔 프록시 요청은 콘솔 프록시 IP 주소에 직접 릴레이되어야 합니다.

단일 IP 주소로 설치하는 경우 Service Provider Admin Portal에서 콘솔 프록시 주소를 사용자 지정할 수 있습니다. 예를 들어 VMware Cloud Director 장치의 경우, 콘솔 프록시 주소를 `vcloud.example.com:8443`으로 사용자 지정해야 합니다.

네트워크 시간 서비스

NTP 같은 네트워크 시간 서비스를 사용하여 데이터베이스 서버를 포함한 모든 VMware Cloud Director 서버의 클럭을 동기화해야 합니다. 동기화된 서버의 클럭 간에 허용되는 최대 드리프트는 2초입니다.

VMware Cloud Director 장치 배포의 경우 전송 공유에 사용된 NFS 서버가 NTP와 같은 네트워크 시간 서비스를 사용하여 해당 클럭을 VMware Cloud Director 장치의 클럭과 동기화해야 합니다. 동기화되는 서버의 클럭 간의 최대 허용 가능 편차는 2초입니다.

서버 시간대

전송 공유에 사용된 NFS 서버 및 데이터베이스 서버를 포함한 모든 VMware Cloud Director 서버는 동일한 표준 시간대에 있도록 구성해야 합니다.

호스트 이름 확인

설치하고 구성하는 동안 지정하는 모든 호스트 이름은 정규화된 도메인 이름이나 정규화되지 않은 호스트 이름의 정방향 및 역방향 조회를 사용하여 DNS로 확인할 수 있어야 합니다. 예를 들어 이름이 `vcloud.example.com`인 호스트의 경우 VMware Cloud Director 호스트에서 다음 명령을 모두 성공해야 합니다.

```
nslookup vcloud
nslookup vcloud.example.com
```

또한 `vcloud.example.com` 호스트의 IP 주소가 `192.168.1.1`인 경우 다음 명령은 `vcloud.example.com`을 반환해야 합니다.

```
nslookup 192.168.1.1
```

장치에 대해 `eth0` IP 주소의 역방향 DNS 조회가 필요합니다. 환경에서 다음 명령이 성공해야 합니다.

```
host -W 15 -R 1 -T <eth0-IP-address>
```

네트워크 보안 요구 사항

VMware Cloud Director의 보안 작업을 수행하려면 보안 네트워크 환경이 필요합니다. VMware Cloud Director 설치를 시작하기 전에 이 네트워크 환경을 구성하고 테스트합니다.

모든 VMware Cloud Director 서버를 안전하고 모니터링되는 네트워크에 연결합니다.

VMware Cloud Director에 사용되는 네트워크 포트 및 프로토콜에 대한 자세한 내용은 [VMware Ports and Protocols](#)를 참조하십시오.

VMware Cloud Director 네트워크 연결에는 다음과 같은 몇 가지 추가 요구 사항이 있습니다.

- VMware Cloud Director를 공용 인터넷에 직접 연결하지 마십시오. 항상 방화벽을 사용하여 VMware Cloud Director 네트워크 연결을 보호해야 합니다. 포트 443(HTTPS)만 들어오는 연결에 열려 있어야 합니다. 필요한 경우 들어오는 연결을 위해 포트 22(SSH) 및 80(HTTP)을 열 수도 있습니다. 또한 cell-management-tool은 셀의 루프백 주소에 액세스해야 합니다. JMX에 대한 요청(포트8999)을 포함하여 공용 네트워크의 다른 모든 수신 트래픽은 방화벽에서 거부되어야 합니다.

VMware Cloud Director 호스트에서 들어오는 패킷을 허용해야 하는 포트에 대한 자세한 내용은 [VMware Ports and Protocols](#)를 참조하십시오.

- 내보내는 연결에 사용되는 포트는 공용 네트워크에 연결하지 마십시오.

VMware Cloud Director 호스트에서 나가는 패킷을 허용해야 하는 포트에 대한 자세한 내용은 [VMware Ports and Protocols](#)를 참조하십시오.

- 버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)을 참조하십시오.

- 전용 개인 네트워크를 통해 VMware Cloud Director 서버와 다음의 서버 사이에 트래픽을 라우팅합니다.

- VMware Cloud Director 데이터베이스 서버
- RabbitMQ
- Cassandra

- 가능한 경우 VMware Cloud Director 서버, vSphere 및 NSX 사이의 트래픽은 전용 개인 네트워크를 통해 라우팅합니다.

- 제공자 네트워크를 지원하는 가상 스위치 및 분산 가상 스위치는 서로 격리되어야 합니다. 해당 스위치는 동일한 계층 2 물리적 네트워크 세그먼트를 공유할 수 없습니다.

- 전송 서비스 스토리지에 NFSv4를 사용합니다. 가장 일반적인 NFS 버전인 NFSv3은 일부 구성에서 전송 중인 데이터에 대한 스니핑 또는 변조를 허용할 수 있는 전송 중 암호화를 제공하지 않습니다. NFSv3에 내재된 위협은 SANS 백서 [신뢰할 수 있는 환경과 신뢰할 수 없는 환경에서의 NFS 보안](#)에 설명되어 있습니다. VMware Cloud Director 전송 서비스 구성 및 보안에 대한 자세한 내용은 VMware 기술 자료 문서 [2086127](#)에서 확인할 수 있습니다.

VMware Cloud Director 장치의 배포, 업그레이드 및 관리

3

버전 9.7부터는 VMware Cloud Director 장치에 고가용성 기능이 있는 내장형 PostgreSQL 데이터베이스가 포함됩니다. VMware Cloud Director 장치를 배포, 업그레이드 또는 마이그레이션할 때 관리, 모니터링, 업데이트 적용 또는 문제 해결 작업을 수행할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 장치 배포 및 데이터베이스 고가용성 구성
- VMware Cloud Director 장치 배포 준비
- VMware Cloud Director 장치의 배포 및 초기 구성
- VMware Cloud Director 장치 업그레이드 및 마이그레이션
- VMware Cloud Director 업그레이드 후 작업
- VMware Cloud Director 장치 관리
- VMware Cloud Director 장치 데이터베이스 클러스터 상태 모니터링
- VMware Cloud Director 장치 데이터베이스 클러스터 복구
- 장치 문제 해결

장치 배포 및 데이터베이스 고가용성 구성

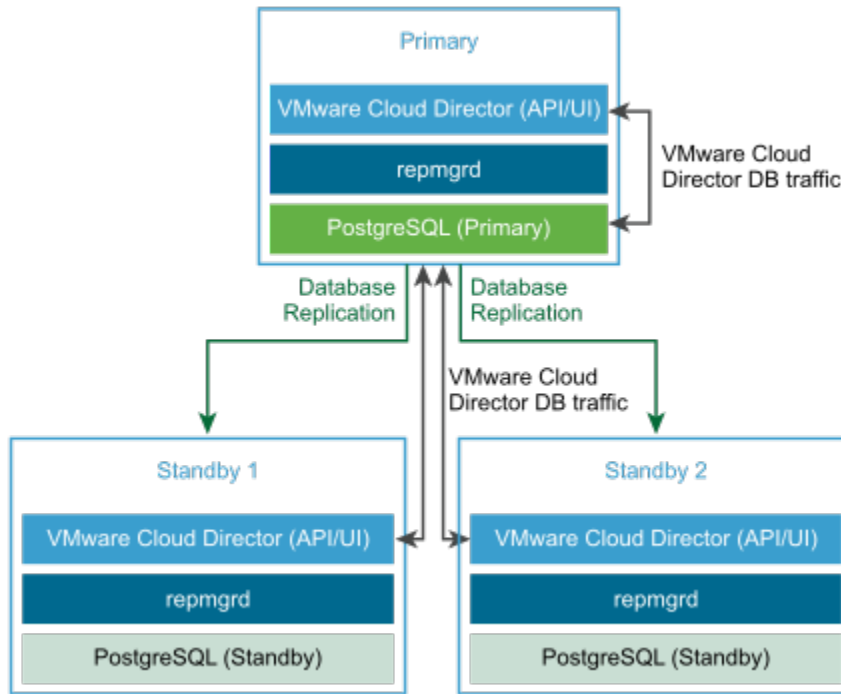
VMware Cloud Director 장치에는 내장형 PostgreSQL 데이터베이스가 포함됩니다. 내장형 PostgreSQL 데이터베이스에는 PostgreSQL 서버의 클러스터에 고가용성(HA) 기능을 제공하는 Replication Manager(repmgr) 도구 집합이 포함되어 있습니다. VMware Cloud Director 데이터베이스에 페일오버 기능을 제공하는 데이터베이스 HA 클러스터를 사용하여 장치 배포를 생성할 수 있습니다.

VMware Cloud Director 장치는 기본 셀, 대기 셀 또는 VMware Cloud Director 애플리케이션 셀로 배포할 수 있습니다. vSphere Client를 사용하여 VMware Cloud Director 장치 배포, VMware OVF Tool을 사용하여 VMware Cloud Director 장치 배포 또는 HTTPS 및 콘솔 프록시 통신을 위해 서명된 와일드카드 인증서를 사용하여 VMware Cloud Director 장치 배포 항목을 참조하십시오.

VMware Cloud Director 데이터베이스에 대해 HA를 구성하려면 서버 그룹을 만들 때 VMware Cloud Director 장치의 기본 인스턴스 1개와 대기 인스턴스 2개를 배포하여 데이터베이스 HA 클러스터를 구성할 수 있습니다. 애플리케이션 셀을 추가로 배포하여 서버 그룹을 가로로 확장할 수 있습니다. 그림 3-1.

VMware Cloud Director 장치 데이터베이스 HA 클러스터 그림을 참조하십시오.

그림 3-1. VMware Cloud Director 장치 데이터베이스 HA 클러스터



데이터베이스 HA를 포함하여 VMware Cloud Director 장치 배포 생성

데이터베이스 HA 구성과 함께 VMware Cloud Director 서버 그룹을 생성하려면 다음 워크플로를 수행합니다.

1 VMware Cloud Director 장치를 기본 셀로 배포합니다.

기본 셀은 VMware Cloud Director 서버 그룹의 첫 번째 구성원입니다. 내장형 데이터베이스는 VMware Cloud Director 데이터베이스로 구성됩니다. 데이터베이스 이름은 `vcloud`이고 데이터베이스 사용자는 `vcloud`입니다.

2 기본 셀이 가동되어 실행 중인지 확인합니다.

- VMware Cloud Director 서비스 상태를 확인하려면 **시스템 관리자** 자격 증명을 사용하여 `https://primary_eth0_ip_address/provider`의 VMware Cloud Director Service Provider Admin Portal에 로그인합니다.
- PostgreSQL 데이터베이스 상태를 확인하려면 `https://primary_eth1_ip_address:5480`에서 장치 관리 사용자 인터페이스에 **루트**로 로그인합니다.

기본 노드의 상태는 실행 중이어야 합니다.

3 VMware Cloud Director 장치의 인스턴스 2개를 대기 셀로 배포합니다.

내장형 데이터베이스는 복제 모드에서 기본 데이터베이스를 사용하여 구성됩니다.

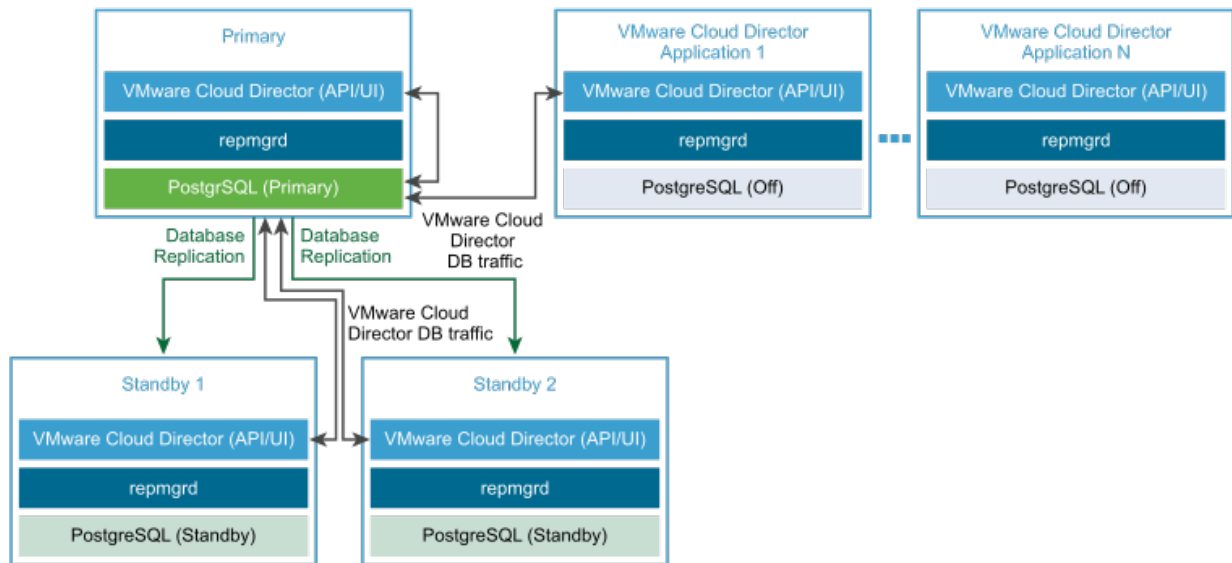
참고 초기 대기 장치 배포 후 Replication Manager는 데이터베이스를 기본 장치 데이터베이스와 동기화하기 시작합니다. 이 시간 동안 VMware Cloud Director 데이터베이스와 VMware Cloud Director UI는 사용할 수 없습니다.

- 4 HA 클러스터의 모든 셀이 실행 중인지 확인합니다.

VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기의 내용을 참조하십시오.

- 5 (선택 사항) 하나 이상의 VMware Cloud Director 장치 인스턴스를 VMware Cloud Director 애플리케이션 셀로 배포합니다.

내장형 데이터베이스는 사용되지 않습니다. VMware Cloud Director 애플리케이션 셀이 기본 데이터베이스에 연결됩니다.



참고 클러스터가 자동 페일오버에 대해 구성되어 있다면 하나 이상의 추가 셀을 배포한 후 장치 API를 사용하여 클러스터 페일오버 모드를 Automatic으로 재설정해야 합니다. VMware Cloud Director 장치 API를 참조하십시오. 새 셀에 대한 기본 페일오버 모드는 Manual입니다. 클러스터의 노드 전체에서 페일오버 모드가 일관되지 않은 경우 클러스터 페일오버 모드는 Indeterminate입니다. Indeterminate 모드는 이전 기본 셀 이후 노드와 기타 노드 간에 일관성 없는 클러스터 상태를 초래할 수 있습니다. 클러스터 페일오버 모드를 보려면 VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기의 내용을 참조하십시오.

데이터베이스 HA 없이 VMware Cloud Director 장치 배포 생성

참고 기본 셀이 하나 있고 대기 셀 또는 애플리케이션 셀이 없는 VMware Cloud Director 클러스터를 배포할 수 있습니다. 단일 셀 배포는 데이터베이스 관점에서 단일 실패 소스이기 때문에 VMware는 운영 환경에서 단일 셀 배포를 지원하지 않습니다. 단일 셀 배포는 성능 또는 안정성 관련 문제에 대한 지원을 받을 수 없습니다.

데이터베이스 HA 구성 없이 VMware Cloud Director 서버를 생성하려면 다음 워크플로를 수행합니다.

1 VMware Cloud Director 장치를 기본 셀로 배포합니다.

기본 셀은 VMware Cloud Director 서버 그룹의 첫 번째 구성원입니다. 내장형 데이터베이스는 VMware Cloud Director 데이터베이스로 구성됩니다. 데이터베이스 이름은 `vcloud`이고 데이터베이스 사용자는 `vcloud`입니다.

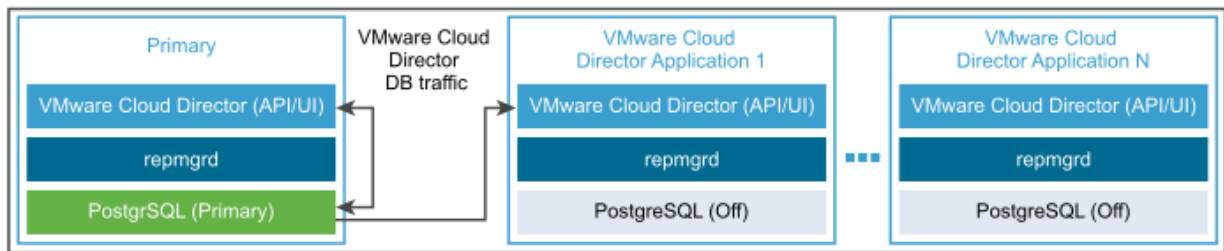
2 기본 셀이 가동되어 실행 중인지 확인합니다.

- a VMware Cloud Director 서비스 상태를 확인하려면 **시스템 관리자** 자격 증명을 사용하여 `https://primary_eth0_ip_address/provider`의 VMware Cloud Director Service Provider Admin Portal에 로그인합니다.
- b PostgreSQL 데이터베이스 상태를 확인하려면 `https://primary_eth1_ip_address:5480`에서 장치 관리 사용자 인터페이스에 **루트**로 로그인합니다.

기본 노드의 상태는 실행 중이어야 합니다.

3 (선택 사항) 하나 이상의 VMware Cloud Director 장치 인스턴스를 VMware Cloud Director 애플리케이션 셀로 배포합니다.

내장형 데이터베이스는 사용되지 않습니다. VMware Cloud Director 애플리케이션 셀이 기본 데이터베이스에 연결됩니다.



VMware Cloud Director 장치의 자동 페일오버

VMware Cloud Director 10.1부터 기본 데이터베이스 서비스가 실패할 경우 VMware Cloud Director를 사용하도록 설정하여 새 기본으로 자동 페일오버를 수행할 수 있습니다.

자동 페일오버를 사용하면 기본 데이터베이스 서비스가 어떤 이유로든 기능을 수행하지 못하는 경우 관리자가 페일오버 작업을 시작하지 않아도 됩니다. 기본적으로 페일오버 모드는 수동으로 설정됩니다.

VMware Cloud Director 장치 API를 사용하여 페일오버 모드를 자동 또는 수동으로 설정할 수 있습니다. "VMware Cloud Director 장치 API 스키마 참조"를 참조하십시오.

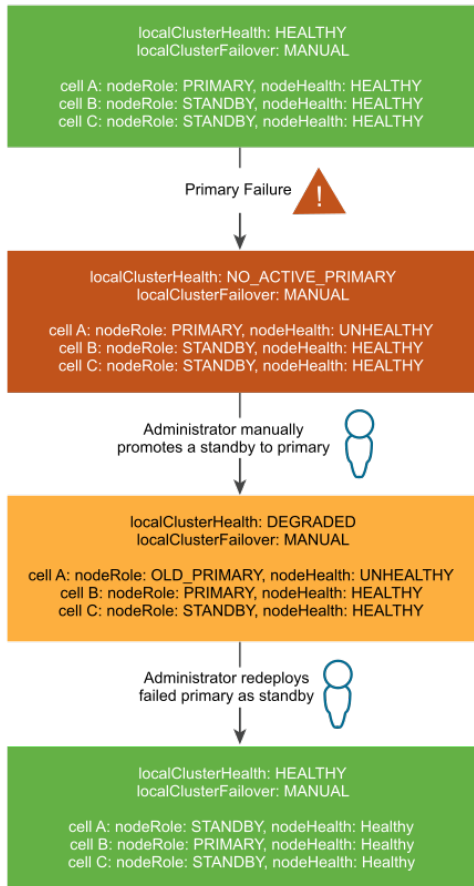
참고 클러스터가 자동 페일오버에 대해 구성되어 있다면 하나 이상의 추가 셀을 배포한 후 장치 API를 사용하여 클러스터 페일오버 모드를 Automatic으로 재설정해야 합니다. VMware Cloud Director 장치 API를 참조하십시오. 새 셀에 대한 기본 페일오버 모드는 Manual입니다. 클러스터의 노드 전체에서 페일오버 모드가 일관되지 않은 경우 클러스터 페일오버 모드는 Indeterminate입니다. Indeterminate 모드는 이전 기본 셀 이후 노드와 기타 노드 간에 일관성 없는 클러스터 상태를 초래할 수 있습니다. 클러스터 페일오버 모드를 보려면 VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기의 내용을 참조하십시오.

환경에 두 개 이상의 활성 대기 셀이 있는 경우 기본 데이터베이스 장애가 발생하면 데이터베이스 페일오버가 자동으로 시작됩니다. 페일오버 후에는 새 기본 데이터베이스를 업데이트할 수 있도록 하나 이상의 활성 대기가 있어야 합니다. 정상적인 상황에서는 VMware Cloud Director 장치 배포에 항상 두 개 이상의 활성 대기가 있어야 합니다. 기본 및 실패 대기 중 하나의 프로모션 등으로 짧은 기간 동안 활성 대기가 하나만 있는 경우 실패한 이전 기본을 가능한 한 빨리 새 대기로 바꾸어야 합니다.

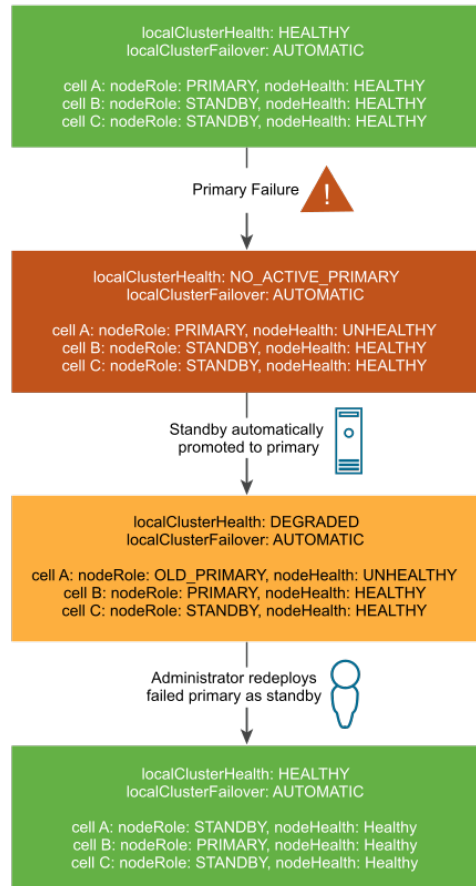
활성 기본 셀과 두 개 이상의 활성 대기 셀이 있는 경우 클러스터가 Healthy 상태에 있는 것으로 간주됩니다. 활성 기본과 하나의 활성 대기만 있는 경우 클러스터가 Degraded 상태에 있습니다. 클러스터가 Degraded 상태에 있는 동안 다른 데이터베이스 장애가 발생하는 경우 다른 대기가 온라인 상태가 될 때까지 기본을 업데이트할 수 없습니다. 기본 데이터베이스를 업데이트할 수 없는 경우 기본 데이터베이스에서 스트리밍 복제를 처리할 하나 이상의 활성 대기가 있을 때까지 VMware Cloud Director 셀이 데이터베이스를 업데이트할 수 없기 때문에 VMware Cloud Director를 사용할 수 없습니다. Healthy 및 Degraded 클러스터의 개념은 수동 페일오버를 사용하도록 설정하든 자동 페일오버를 사용하도록 설정하든 동일합니다.

그림 3-2. 수동 및 자동 VMware Cloud Director 장치 페일오버

Manual VMware Cloud Director Appliance Failover



Automatic VMware Cloud Director Appliance Failover



실패한 기본 셀의 자동 펜싱

기본 셀 실패 후 새 기본 셀이 승격되는 경우 VMware Cloud Director는 다시 시작되지 않도록 이전 기본 셀을 자동으로 펜싱합니다.

페일오버의 경우 실패한 기본 데이터베이스가 새 기본 셀이 승격된 후 다시 시작되면 VMware Cloud Director는 이전 기본 셀을 자동으로 펜싱합니다. 이러한 자동화는 두 활성 데이터베이스가 서로 분리될 수 있는 분할 브레인(split-brain) 증상을 방지합니다. 펜싱 자동화는 이전 기본 노드에서 vPostgres 서비스를 중지하고 비활성화합니다. 그런 다음 실패한 기본 셀을 대기 셀로 다시 배포하여 클러스터 상태를 Healthy으로 복원할 수 있습니다.

클러스터 상태 및 페일오버 모드 보기에 대한 자세한 내용은 [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#) 항목을 참조하십시오.

VMware Cloud Director 장치 배포 준비

VMware Cloud Director 장치를 배포하기 전에 환경을 준비해야 합니다.

VMware Cloud Director 장치를 위한 전송 서버 스토리지 준비

NFS 또는 기타 공유 스토리지 볼륨을 VMware Cloud Director 서버 그룹의 모든 서버에서 액세스할 수 있도록 설정해야 합니다. VMware Cloud Director는 장치 클러스터 관리를 위해 그리고 외부에서 게시 또는 구독하는 업로드, 다운로드 및 카탈로그 항목을 위한 임시 스토리지를 제공하기 위해 전송 서버 스토리지를 사용합니다.

중요 VMware Cloud Director 장치는 NFS 유형의 공유 스토리지만 지원합니다. 장치 배포 프로세스에는 NFS 공유 전송 서버 스토리지를 마운트하는 단계가 포함됩니다. 또한 VMware Cloud Director 장치는 배포 중에 디렉토리 사용 권한 및 소유권을 비롯한 NFS 공유에 대한 대부분의 세부 정보를 확인합니다. 올바른 NFS 마운트 지점이 있는지 그리고 VMware Cloud Director 장치 인스턴스에서 이러한 마운트 지점에 액세스할 수 있는지 확인해야 합니다.

서버 그룹의 각 구성원은 이 볼륨을 동일한 마운트 지점(/opt/vmware/vcloud-director/data/transfer)에 마운트합니다. 이 볼륨의 공간은 다음과 같은 여러 가지 방식으로 사용됩니다.

- 전송하는 동안 업로드 및 다운로드가 이 스토리지를 차지합니다. 전송이 완료되면 업로드 및 다운로드가 스토리지에서 제거됩니다. 60분 동안 진행되지 않은 전송은 만료된 것으로 표시되고 시스템에 의해 정리됩니다. 전송되는 이미지가 클 수 있으므로 이 용도로 사용하려면 적어도 수백 기가바이트를 할당하는 것이 좋습니다.
- 외부에 게시되고 게시된 콘텐츠에 대한 캐싱을 사용할 수 있는 카탈로그의 카탈로그 항목은 이 스토리지를 차지합니다. 외부에 게시되지만 캐싱을 사용할 수 없는 카탈로그의 항목은 이 스토리지를 차지하지 않습니다. 클라우드의 조직에서 외부에 게시되는 카탈로그를 만들 수 있도록 설정하는 경우에는 수백 또는 수천 개의 카탈로그 항목이 이 볼륨의 공간을 필요로 한다고 가정할 수 있습니다. 각 카탈로그 항목의 크기는 압축된 OVF 형식의 가상 시스템 크기입니다.
- VMware Cloud Director는 장치 데이터베이스 백업을 전송 공유의 pgdb-backup 디렉토리에 저장합니다. 이러한 백업 번들에 상당한 공간이 사용될 수 있습니다.
- 다중 셀 로그 번들 수집기는 이 공간을 차지합니다.
- 장치 노드 데이터 및 response.properties 파일은 이 공간을 차지합니다.

참고 전송 서버 스토리지의 볼륨에는 향후 확장을 위한 용량이 있어야 합니다.

참고 NFS 다운타임으로 인해 VMware Cloud Director 장치 클러스터 기능이 오작동할 수 있습니다. NFS가 다운되었거나 NFS에 연결할 수 없으면 장치 관리 UI가 응답하지 않습니다. 실패한 기본 셀 펜싱, 전환, 대기 셀 승격 등과 같은 기능도 영향을 받을 수 있습니다.

참고 NFS에 Ubuntu 또는 Debian 기반 Linux 배포를 사용하는 경우 데이터베이스 백업 생성이 실패할 수 있습니다.

공유 스토리지 옵션

기존 Linux 기반 NFS 서버 또는 Microsoft Windows Server와 같은 기타 솔루션, VMware vSAN 파일 서비스 NFS 기능 등은 공유 스토리지를 제공할 수 있습니다. vSAN 7.0부터는 vSAN 파일 서비스 기능을 통해 NFS 3.0 및 NFS 4.1 프로토콜을 사용하여 NFS 공유를 내보낼 수 있습니다. vSAN 파일 서비스에 대한 자세한 내용은 [VMware vSphere 제품 설명서](#)의 "VMware vSAN 관리" 가이드를 참조하십시오.

NFS 서버 구성을 위한 요구 사항

NFS 서버 구성을 위해서는 VMware Cloud Director가 NFS 기반 전송 서버 스토리지 위치에 파일을 쓰고 읽을 수 있어야 한다는 구체적인 요구 사항이 있습니다. 이로 인해 **vcloud** 사용자는 표준 클라우드 운영을 수행할 수 있고 **root** 사용자는 다중 셀 로그 수집을 수행할 수 있습니다.

- NFS 서버의 내보내기 목록은 VMware Cloud Director 서버 그룹의 각 서버 멤버가 내보내기 목록에서 식별된 공유 위치에 대한 읽기/쓰기 액세스 권한을 갖도록 허용해야 합니다. 이 기능을 사용하면 **vcloud** 사용자가 공유 위치에 파일을 쓰고 읽을 수 있습니다.
- NFS 서버는 VMware Cloud Director 서버 그룹의 각 서버에서 **root** 계정으로 공유 위치에 대한 읽기/쓰기 액세스 권한을 허용해야 합니다. 이 기능을 사용하면 `vmware-vcd-support` 스크립트를 다중 셀 옵션과 함께 사용하여 단일 번들에서 모든 셀의 로그를 한 번에 수집할 수 있습니다. 이 공유 위치에 대한 NFS 내보내기 구성에서 `no_root_squash`를 사용하여 이 요구 사항을 충족할 수 있습니다.

Linux NFS 서버 예제

예를 들어, Linux NFS 서버에 VMware Cloud Director 서버 그룹의 전송 공간으로 `vCDspace`라는 디렉토리가 있고 해당 위치가 `/nfs/vCDspace`인 경우 이 디렉토리를 내보내려면 소유권과 사용 권한이 **root:root** 및 **750**이어야 합니다. `vCD-Cell1-IP`, `vCD-Cell2-IP`, `vCD-Cell3-IP`라는 3개 셀의 공유 위치에 대한 읽기/쓰기 액세스 권한을 허용하는 메서드는 `no_root_squash` 메서드입니다. `/etc/exports` 파일에 다음 줄을 추가해야 합니다.

```
/nfs/vCDspace vCD_Cell1_IP_Address(rw, sync, no_subtree_check, no_root_squash)
/nfs/vCDspace vCD_Cell2_IP_Address(rw, sync, no_subtree_check, no_root_squash)
/nfs/vCDspace vCD_Cell3_IP_Address(rw, sync, no_subtree_check, no_root_squash)
```

내보내기 줄에서 각 셀 IP 주소와 바로 다음 왼쪽 괄호 사이에 공백이 없어야 합니다. 셀이 공유 위치에 데이터를 쓰는 동안 NFS 서버가 재부팅되는 경우, 내보내기 구성에서 `sync` 옵션을 사용하면 공유 위치에서 데이터가 손상되지 않습니다. 내보내기 구성에서 `no_subtree_check` 옵션을 사용하면 파일 시스템의 하위 디렉토리를 내보낼 때 안정성이 향상됩니다.

VMware Cloud Director 서버 그룹의 각 서버에 대해 NFS 서버의 `/etc/exports` 파일에 해당 항목이 있어야 NFS 공유를 모두 마운트할 수 있습니다. NFS 서버에서 `/etc/exports` 파일을 변경한 후 `exportfs -a`를 실행하여 모든 NFS 공유를 다시 내보냅니다.

VMware Cloud Director용 NSX Data Center for vSphere 설치 및 구성

VMware Cloud Director 설치 환경에서 NSX Data Center for vSphere의 네트워크 리소스를 사용하려면 경우, NSX Data Center for vSphere를 설치하여 구성하고 VMware Cloud Director 설치에 포함하려는 각 vCenter Server 인스턴스에 고유한 NSX Manager 인스턴스를 연결해야 합니다.

NSX Manager는 NSX Data Center for vSphere 다운로드에 포함되어 있습니다. VMware Cloud Director 및 기타 VMware 제품 간 호환성에 대한 최신 정보는 "VMware 제품 상호 운용성 매트릭스" (<http://partnerware.vmware.com>)를 참조하십시오. 네트워크 요구 사항에 대한 자세한 내용은 [VMware Cloud Director에 대한 네트워크 구성 요구 사항](#)을 참조하십시오.

중요 VMware Cloud Director를 새로 설치할 경우에만 이 절차가 적용됩니다. VMware Cloud Director의 기존 설치를 업그레이드할 경우 [Linux에서 VMware Cloud Director 업그레이드](#)를 참조하십시오.

사전 요구 사항

각 vCenter Server 시스템이 NSX Manager 설치를 위한 전제 조건을 충족하는지 확인합니다.

절차

- 1 NSX Manager 가상 장치에 대한 설치 작업을 수행합니다.

"NSX 설치 가이드"를 참조하십시오.

- 2 설치한 NSX Manager 가상 장치에 로그인하여 설치 중에 지정한 설정을 확인합니다.

- 3 설치한 NSX Manager 가상 장치를 계획한 VMware Cloud Director 설치에서 VMware Cloud Director에 추가하려는 vCenter Server 시스템과 연결합니다.

- 4 연결된 NSX Manager 인스턴스에서 VXLAN 지원을 구성합니다.

VMware Cloud Director에서는 VXLAN 네트워크 풀을 생성하여 제공자 VDC에 네트워크 리소스를 제공합니다. 연결된 NSX Manager에 VXLAN 지원이 구성되지 않은 경우 제공자 VDC에서 네트워크 풀 오류를 표시하고 사용자는 다른 유형의 네트워크 풀을 만들어 제공자 VDC와 연결해야 합니다. VXLAN 지원 구성에 대한 자세한 내용은 "NSX 관리 가이드"의 내용을 참조하십시오.

- 5 (선택 사항) 시스템의 Edge 게이트웨이가 분산 라우팅을 제공하도록 하려면 NSX Controller 클러스터를 설정합니다.

"NSX 관리 가이드"를 참조하십시오.

VMware Cloud Director용 NSX-T Data Center 설치 및 구성

VMware Cloud Director 설치 환경에서 NSX-T Data Center의 네트워크 리소스를 사용하려는 경우, NSX-T Data Center를 설치하고 구성해야 합니다.

중요 NSX-T Data Center 개체 및 도구를 구성하려면 간소화된 정책 UI 및 간소화된 UI에 해당하는 정책 API를 사용합니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"에서 NSX-T Manager 개요를 참조하십시오.

VMware Cloud Director와 기타 VMware 제품 간 호환성에 대한 최신 정보는 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

네트워크 요구 사항에 대한 자세한 내용은 [VMware Cloud Director에 대한 네트워크 구성 요구 사항](#)을 참조하십시오.

VMware Cloud Director를 새로 설치할 경우에만 이 절차가 적용됩니다. VMware Cloud Director의 기존 설치를 업그레이드할 경우 [Linux에서 VMware Cloud Director 업그레이드](#)를 참조하십시오.

사전 요구 사항

NSX-T Data Center를 숙지합니다.

절차

- 1 NSX-T Manager 가상 장치를 배포하고 구성합니다.

NSX-T Manager 배포에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드" 항목을 참조하십시오.

- 2 네트워킹 요구 사항을 기반으로 전송 영역을 생성합니다.

전송 영역 생성에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드" 항목을 참조하십시오.

참고

- 3 Edge 노드 및 Edge 클러스터를 배포하고 구성합니다.

NSX Edge 생성에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드" 항목을 참조하십시오.

- 4 ESXi 호스트 전송 노드를 구성합니다.

관리되는 호스트 전송 노드 구성에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드" 항목을 참조하십시오.

- 5 Tier-0 게이트웨이를 생성합니다.

Tier-0 생성에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드" 항목을 참조하십시오.

다음에 수행할 작업

VMware Cloud Director를 설치한 후 다음을 수행할 수 있습니다.

- 1 클라우드에 NSX-T Manager 인스턴스를 등록합니다.

NSX-T Manager 인스턴스 등록에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드" 항목을 참조하십시오.

- 2 NSX-T Data Center 전송 영역에서 지원하는 네트워크 풀을 생성합니다.

NSX-T Data Center 전송 영역에서 지원하는 네트워크 풀을 생성하는 방법에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드" 항목을 참조하십시오.

- 3 Tier-0 게이트웨이를 외부 네트워크로 가져옵니다.

NSX-T Data Center Tier-0 논리적 라우터가 지원하는 외부 네트워크를 추가하는 방법에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드" 항목을 참조하십시오.

VMware Cloud Director 장치의 배포 및 초기 구성

하나 이상의 VMware Cloud Director 장치 인스턴스를 배포하여 VMware Cloud Director 서버 그룹을 만들 수 있습니다. vSphere Client 또는 VMware OVF Tool을 사용하여 VMware Cloud Director 장치를 배포합니다.

중요 하나의 서버 그룹에서 Linux에 설치된 VMware Cloud Director 및 VMware Cloud Director 장치 배포의 혼합은 지원되지 않습니다.

VMware Cloud Director 장치는 VMware Cloud Director 서비스 실행에 최적화되어 미리 구성된 가상 시스템입니다.

장치는 VMware Cloud Director-*v.v.v.v-**nnnnnn**_OVF10.ova* 형식의 이름으로 배포됩니다. 여기서 *v.v.v.v*는 제품 버전을 나타내고 *nnnnnn*은 빌드 번호를 나타냅니다. 예: VMware Cloud Director-9.7.0.0-9229800_OVA10.ova.

VMware Cloud Director 장치 패키지에는 다음 소프트웨어가 포함됩니다.

- VMware Photon™ OS
- VMware Cloud Director 서비스 그룹
- PostgreSQL 10

기본-소 및 대기-소 VMware Cloud Director 장치 크기는 랩 또는 테스트 시스템에 적합합니다. 기본-대 및 대기-대 크기는 운영 시스템에 대한 최소 크기 조정 요구 사항을 충족합니다. 워크로드에 따라 리소스를 추가해야 할 수도 있습니다.

중요 VMware Cloud Director 장치에서 타사 구성 요소를 설치하는 기능은 지원되지 않습니다. [VMware 제품 상호 운용성 매트릭스](#)에 따라 지원되는 VMware 구성 요소만 설치할 수 있습니다. 예를 들어 지원되는 버전의 VMware vRealize® Operations Manager™ 또는 VMware vRealize® Log Insight™ 모니터링 에이전트를 설치할 수 있습니다.

장치 데이터베이스 구성

버전 9.7부터는 VMware Cloud Director 장치에고가용성(HA) 기능이 있는 내장형 PostgreSQL 데이터베이스가 포함됩니다. 데이터베이스 HA 클러스터로 장치 배포를 생성하려면 VMware Cloud Director 장치의 1개 인스턴스는 기본 셀로 배포하고 2개 인스턴스는 대기 셀로 배포해야 합니다. 서버 그룹에 VMware Cloud Director 장치의 추가 인스턴스를 vCD 애플리케이션 셀로 배포할 수 있으며, 이 셀은 내장형 데이터베이스 없이 VMware Cloud Director 서비스 그룹만 실행합니다. vCD 애플리케이션 셀은 기본 셀의 데이터베이스에 연결됩니다. [장치 배포 및 데이터베이스고가용성 구성](#)의 내용을 참조하십시오.

기본적으로 VMware Cloud Director 장치는 복제를 비롯한 데이터베이스 연결에 대해 더 이상 사용되지 않는 SSL 대신 TLS를 사용합니다. 이 기능은 자체 서명된 PostgreSQL 인증서를 사용하여 배포 직후 활성화됩니다. CA(인증 기관)의 서명된 인증서를 사용하려면 [자체 서명된 내장형 PostgreSQL 및 VMware Cloud Director 장치 관리 UI 인증서 교체](#) 항목을 참조하십시오.

참고 VMware Cloud Director 장치는 외부 데이터베이스를 지원하지 않습니다.

어플라이언스 네트워크 구성

버전 9.7부터는 VMware Cloud Director 장치가 2개의 네트워크(eth0 및 eth1)로 배포되기 때문에 HTTP 트래픽을 데이터베이스 트래픽과 격리할 수 있습니다. 서로 다른 서비스는 해당 네트워크 인터페이스 중 하나 또는 둘 다를 수신 대기합니다.

참고 eth0 및 eth1 네트워크는 별도의 서브넷에 배치해야 합니다.

서비스	eth0의 포트	eth1의 포트
SSH	22	22
HTTP	80	해당 없음
HTTPS	443	해당 없음
PostgreSQL	해당 없음	5432
관리 UI	5480	5480
콘솔 프록시	8443	해당 없음
JMX	8998, 8999	해당 없음
JMS/ActiveMQ	61616	해당 없음

VMware Cloud Director 장치를 생성한 후 vSphere 네트워킹 기능을 사용하여 새 NIC(네트워크 인터페이스 카드)를 추가할 수 있습니다. "vSphere 가상 시스템 관리" 가이드에서 [가상 시스템에 네트워크 어댑터 추가](#) 정보를 참조하십시오.

VMware Cloud Director 장치는 iptables를 사용하여 방화벽 규칙의 사용자 지정을 지원합니다. 사용자 지정 iptables 규칙을 추가하려면 /etc/systemd/scripts/iptables 파일의 끝에 자신의 구성 데이터를 추가하면 됩니다.

버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)의 내용을 참조하십시오.

VMware Cloud Director 장치 크기 조정 지침

필요에 따라 VMware Cloud Director 장치 기반 서버 구성이 다르고 VMware Cloud Director 가상 장치 인스턴스의 크기가 다를 수 있습니다.

개요

기본 셀 장애가 발생할 경우 클러스터가 자동화된 페일오버를 지원할 수 있도록 최소 VMware Cloud Director 배포는 기본 셀 1개와 대기 셀 2개로 구성되어야 합니다. 어떤 이유로든 셀 중 하나가 오프라인 상태가 되는 장애 시나리오에서 환경을 계속 사용할 수 있습니다. 대기 장애가 발생하면 장애가 발생한 셀을 다시 배포할 때까지 클러스터는 완전히 작동하는 상태에서 성능이 약간 저하되어 작동합니다. [장치 배포 및 데이터베이스 고가용성 구성](#)의 내용을 참조하십시오.

VMware Cloud Director 장치에는 배포 중에 선택할 수 있는 네 가지 크기인 소형, 중형, 대형 및 초대형 (VVD)이 있습니다. 소형 장치 크기는 시험 평가에 적합하며 이 문서에서는 소형 장치 구성에 대한 지침을 제공하지 않습니다. 크기 조정 옵션 테이블은 나머지 옵션에 대한 규격과 운영 환경에 가장 적합한 사용 사례를 제공합니다. 초대형 구성은 [VVD\(VMware Validated Design\) for Cloud Providers](#) 크기 조정 프로파일과 일치합니다.

더 큰 사용자 지정 크기를 생성하기 위해 **시스템 관리자**는 배포된 셀의 크기를 조정할 수 있습니다.

프로덕션 배포에 권장되는 최소 구성은 중형 가상 장치의 3노드 배포입니다.

참고 기본 셀이 하나 있고 대기 셀 또는 애플리케이션 셀이 없는 VMware Cloud Director 클러스터를 배포할 수 있습니다. 단일 셀 배포는 데이터베이스 관점에서 단일 실패 소스이기 때문에 VMware는 운영 환경에서 단일 셀 배포를 지원하지 않습니다. 단일 셀 배포는 성능 또는 안정성 관련 문제에 대한 지원을 받을 수 없습니다.

VMware Cloud Director 장치 크기 조정 옵션

다음 의사 결정 가이드를 사용하여 환경에 맞는 장치 크기를 예상할 수 있습니다.

	중형	대형	초대형(VVD)
권장 사용 사례	시험 또는 소규모 운영 환경	운영 환경	API 통합 및 모니터링을 사용하는 운영
VMware Cloud Director 환경에서 vRealize Operations Management Pack 배포	아니요	아니요	예
VMware Cloud Director에서 Cassandra VM 메트릭 사용 설정	아니요	아니요	예
최대 30분 동안 API에 액세스하는 동시 사용자 또는 클라이언트의 대략적인 수입니다.	< 50	< 100	< 100
관리 VM	5000	5000	15000

구성 정의

참고 VMware Cloud Director 9.7 이상 primary-large 및 standby-large 장치에서는 기본적으로 대형 HA 클러스터 구성에 16개의 vCPU가 필요하지 않습니다. 대형 VMware Cloud Director 장치 구성을 사용하려면 배포 후 기본 및 대기 셀 vCPU를 16으로 수동으로 변경해야 합니다.

	중형	대형	초대형(VVD)
HA 클러스터 구성	기본 셀 1개 + 대기 셀 2개	기본 셀 1개 + 대기 셀 2개 + 애플리케이션 셀 1개	기본 셀 1개 + 대기 셀 2개 + 애플리케이션 셀 2개
vCPU 기본 또는 대기 셀	8	16	24
vCPU 애플리케이션 셀	해당 없음	8	8
RAM 기본 또는 대기 셀	16 GB	24 GB	32 GB
RAM 애플리케이션 셀	해당 없음	8	8
vCPU 대 물리적 코어 비율	1:1	1:1	1:1
기본 및 대기 셀에서 PostgreSQL 사용자 지정	shared_buffers = '3GB'; effective_cache_size = '9GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '8';	shared_buffers = '5GB'; effective_cache_size = '15GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '16';	shared_buffers = '7GB'; effective_cache_size = '21GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes = '24';

시스템 크기가 부족한지 감지하는 방법

VMware Cloud Director 셀에서 CPU 또는 메모리 사용량이 증가하고 높은 수준, 즉 용량에 가까운 수준에서 정체에 도달합니다. VMware Cloud Director 셀도 데이터베이스에 대한 연결이 끊어질 수 있습니다.

시스템 셀 수가 부족한지 감지하는 방법

VMware Cloud Director 셀의 vcloud-container-debug.log 및 cell-runtime.log 파일에 다음과 유사한 항목이 표시됩니다. org.apache.tomcat.jdbc.pool.PoolExhaustedException: [pool-jetty-XXXXX] Timeout: Pool empty. Unable to fetch a connection in 20 seconds, none available. VMware Cloud Director 셀도 데이터베이스에 대한 연결이 끊어질 수 있습니다.

참고 기본 데이터베이스 연결 구성에 따라 모든 구성은 기본, 대기 및 애플리케이션 유형의 최대 6개 셀로 제한됩니다.

장치 크기 조정을 사용자 지정하는 방법

VMware Cloud Director 장치의 크기 조정을 지원되는 구성 중 하나로 사용자 지정하려면 VMware Cloud Director 장치 배포자를 실행한 후 모든 셀에서 이 절차를 따라야 합니다.

- 1 선택한 구성에 필요한 셀 수가 있는지 확인합니다.
- 2 원하는 지원되는 구성 중 하나와 일치하도록 모든 셀의 메모리 및 vCPU를 조정합니다.

중요 RAM과 vCPU의 양은 모든 기본 및 대기 셀에서 동일해야 합니다.

- 3 기본 장치의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 4 사용자를 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

- 5 다음 명령을 실행하여 postgresql.auto.conf 구성 파일을 업데이트합니다.

구성 유형	설명
중형	<pre>psql -c "ALTER SYSTEM set shared_buffers = '3GB';" psql -c "ALTER SYSTEM set effective_cache_size = '9GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '8';"</pre>
대형	<pre>psql -c "ALTER SYSTEM set shared_buffers = '5GB';" psql -c "ALTER SYSTEM set effective_cache_size = '15GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '16';"</pre>
초대형	<pre>psql -c "ALTER SYSTEM set shared_buffers = '7GB';" psql -c "ALTER SYSTEM set effective_cache_size = '21GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '24';"</pre>

- 6 exit 명령을 실행하여 **루트** 사용자로 돌아갑니다.
- 7 vpostgres 프로세스를 다시 시작합니다.

```
systemctl restart vpostgres
```

- 8 사용자를 다시 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

- 9 각 대기 노드에 대해 postgresql.auto.conf 파일을 노드에 복사하고 vpostgres 프로세스를 다시 시작합니다.

- a postgresql.auto.conf를 기본 노드에서 대기 노드로 복사합니다.

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
```

- b vpostgres 프로세스를 다시 시작합니다.

```
systemctl restart vpostgres
```

VMware Cloud Director 장치의 크기 조정을 지원되는 구성 중 하나로 사용자 지정하려면 VMware Cloud Director 장치 배포자를 실행한 후 모든 셀에서 이 절차를 따라야 합니다.

- 1 기본 장치의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 vCPU 정보를 보고 기록해 두려면 다음 명령을 실행합니다.

```
grep -c processor /proc/cpuinfo
```

- 3 RAM 정보를 보고 기록해 두려면 다음 명령을 실행합니다.

아래 보고된 RAM은 KB 단위이며 1024000으로 나누어 GB로 변환해야 합니다.

```
cat /proc/meminfo | grep MemTotal | cut -dk -f1 | awk '{print int($2/1024000)}'
```

- 4 shared_buffers 값은 총 RAM에서 4GB를 뺀 값의 1/4로 계산합니다.

$shared_buffers = 0.25 * (\text{총 RAM} - 4GB)$

- 5 effective_cache_size 값은 총 RAM에서 4GB를 뺀 값의 3/4으로 계산합니다.

$effective_cache_size = 0.75 * (\text{총 RAM} - 4GB)$

- 6 max_worker_processes 값은 vCPU 수로 계산합니다.

- 7 사용자를 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

- 8 다음 명령을 실행하고 계산된 값을 대체하여 postgresql.auto.conf 구성 파일을 업데이트합니다.

```
psql -c "ALTER SYSTEM set shared_buffers = 'shared_buffers value';"
psql -c "ALTER SYSTEM set effective_cache_size = 'effective_cache_size value';"
psql -c "ALTER SYSTEM set work_mem = '8MB';"
psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"
psql -c "ALTER SYSTEM set max_worker_processes= 'max_worker_processes value';"
```

- 9 exit 명령을 실행하여 **루트** 사용자로 돌아갑니다.

- 10 vpostgres 프로세스를 다시 시작합니다.

```
systemctl restart vpostgres
```

- 11 사용자를 다시 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

- 12 각 대기 노드에 대해 postgresql.auto.conf 파일을 노드에 복사하고 vpostgres 프로세스를 다시 시작합니다.

- a postgresql.auto.conf를 기본 노드에서 대기 노드로 복사합니다.

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@standby-node-  
address:/var/vmware/vpostgres/current/pgdata/
```

- b vpostgres 프로세스를 다시 시작합니다.

```
systemctl restart vpostgres
```

VMware Cloud Director 장치 배포를 위한 사전 요구 사항

VMware Cloud Director 장치를 성공적으로 배포하려면 배포를 시작하기 전에 몇 가지 작업과 사전 검사를 수행해야 합니다.

- VMware Cloud Director .ova 파일에 액세스할 수 있는지 확인합니다.
- 기본 장치를 배포하기 전에 NFS 공유 전송 서비스 스토리지를 준비합니다. [Linux에서 VMware Cloud Director를 위한 전송 서버 스토리지 준비](#)의 내용을 참조하십시오.

참고 공유 전송 서비스 스토리지에는 responses.properties 파일이나 appliance-nodes 디렉토리가 없어야 합니다.

- [RabbitMQ AMQP 브로커 설치 및 구성](#).

VMware Cloud Director 장치 배포 방법

- vSphere Client를 사용하여 VMware Cloud Director 장치 배포
- VMware OVF Tool을 사용하여 VMware Cloud Director 장치 배포
- HTTPS 및 콘솔 프록시 통신을 위해 서명된 와일드카드 인증서를 사용하여 VMware Cloud Director 장치 배포

vSphere Client를 사용하여 VMware Cloud Director 장치 배포

vSphere Client(HTML5)를 사용하여 OVF 템플릿으로 VMware Cloud Director 장치를 배포할 수 있습니다. OVF 템플릿을 배포한 후에는 장치 관리 사용자 인터페이스에서 구성을 완료해야 합니다.

VMware Cloud Director 서버 그룹의 첫 번째 구성원을 기본 셀로 배포해야 합니다. VMware Cloud Director 서버 그룹의 후속 구성원은 대기 또는 VMware Cloud Director 애플리케이션 셀로 배포할 수 있습니다. [장치 배포 및 데이터베이스 고가용성 구성](#)의 내용을 참조하십시오.

중요 하나의 서버 그룹에서 Linux에 설치된 VMware Cloud Director 및 VMware Cloud Director 장치 배포의 혼합은 지원되지 않습니다.

데이터베이스 클러스터에 추가 또는 교체용 장치를 추가하는 경우 vCPU 및 RAM이 클러스터에 있는 기존의 기본 및 대기 셀과 일치해야 합니다.

새로 배포된 대기 항목의 OVA 버전은 클러스터의 기존 장치와 동일해야 합니다. 실행 중인 장치의 버전을 보려면 장치 관리 UI에서 정보를 참조하십시오. 장치는 VMware Cloud Director-v.v.v.v-
nnnnnn_OVF10.ova 형식의 이름으로 배포됩니다. 여기서 v.v.v.v는 제품 버전을 나타내고 nnnnnn은 빌드 번호를 나타냅니다. 예: VMware Cloud Director-10.2.0.0-9229800_OVA10.ova.

vSphere에서 OVF 템플릿을 배포하는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리"를 참조하십시오.

또는 VMware OVF Tool을 사용하여 장치를 배포할 수도 있습니다. [VMware OVF Tool을 사용하여 VMware Cloud Director 장치 배포](#)의 내용을 참조하십시오.

참고 VMware Cloud Director에서 VMware Cloud Director 장치를 배포하는 기능은 지원되지 않습니다.

사전 요구 사항

VMware Cloud Director 장치 배포를 위한 [사전 요구 사항](#)의 내용을 참조하십시오.

절차

1 VMware Cloud Director 장치 배포 시작

장치 배포를 시작하려면 vSphere Web Client(Flex) 또는 vSphere Client(HTML5)에서 배포 마법사를 열고 OVF 템플릿을 배포합니다.

2 VMware Cloud Director 기본 장치 구성

기본 장치에 대한 OVF 템플릿을 배포한 후에는 기본 VMware Cloud Director 장치 인스턴스의 장치 관리 사용자 인터페이스에서 구성 단계를 계속해야 합니다.

3 VMware Cloud Director 대기 및 애플리케이션 셀 구성

대기 또는 애플리케이션 셀에 대해 OVF 템플릿을 배포한 후에는 배포하려는 인스턴스의 장치 관리 사용자 인터페이스에서 구성 단계를 계속해야 합니다.

다음에 수행할 작업

- VMware Cloud Director 장치가 콘솔 프록시 서비스에 대해 사용자 지정 포트가 8443인 eth0 NIC를 사용하기 때문에 공용 콘솔 프록시 주소를 구성합니다. [Linux용 VMware Cloud Director에 대한 공개 주소 사용자 지정](#)의 내용을 참조하십시오.

- VMware Cloud Director 서버 그룹에 구성원을 추가하려면 이 절차를 반복합니다.
- 라이선스 키를 입력하려면 VMware Cloud Director Service Provider Admin Portal에 로그인합니다.
- 장치를 처음 부팅하는 동안 생성된 자체 서명된 인증서를 교체하려면 [Linux에 VMware Cloud Director에 대한 CA 서명된 SSL 인증서 키 저장소 생성](#) 작업을 수행하면 됩니다.

VMware Cloud Director 장치 배포 시작

장치 배포를 시작하려면 vSphere Web Client(Flex) 또는 vSphere Client(HTML5)에서 배포 마법사를 열고 OVF 템플릿을 배포합니다.

절차

- 1 vSphere Web Client 또는 vSphere Client에서 인벤토리 개체를 마우스 오른쪽 단추로 클릭하고 **OVF 템플릿 배포**를 클릭합니다.
- 2 VMware Cloud Director .ova 파일의 경로를 입력하고 **다음**을 클릭합니다.
- 3 가상 시스템의 이름을 입력하고 vCenter Server 저장소에서 장치를 배포할 데이터 센터 또는 폴더를 찾아서 선택하고 **다음**을 클릭합니다.
- 4 장치를 배포할 ESXi 호스트 또는 클러스터를 선택하고 **다음**을 클릭합니다.
- 5 템플릿 세부 정보를 검토하고 **다음**을 클릭합니다.
- 6 라이선스 계약을 읽고 동의한 후 **다음**을 클릭합니다.
- 7 배포 유형 및 크기를 선택하고 **다음**을 클릭합니다.

기본-소 및 대기-소 VMware Cloud Director 장치 크기는 랩 또는 테스트 시스템에 적합합니다. 기본-대 및 대기-대 크기는 운영 시스템에 대한 최소 크기 조정 요구 사항을 충족합니다. 워크로드에 따라 리소스를 추가해야 할 수도 있습니다.

옵션	설명
기본-소	<p>RAM이 12GB이고 vCPU가 2개인 장치를 VMware Cloud Director 서버 그룹의 첫 번째 구성원으로 배포합니다.</p> <p>기본 셀에 내장된 데이터베이스는 VMware Cloud Director 데이터베이스로 구성됩니다. 데이터베이스 이름은 vcloud이고 데이터베이스 사용자는 vcloud입니다.</p>
기본-대	<ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 이상 버전은 RAM이 24GB이고 vCPU가 8개인 장치를 VMware Cloud Director 서버 그룹의 첫 번째 구성원으로 배포합니다. ■ VMware Cloud Director 10.2는 RAM이 24GB이고 vCPU가 4개인 장치를 VMware Cloud Director 서버 그룹의 첫 번째 구성원으로 배포합니다. <p>기본 셀에 내장된 데이터베이스는 VMware Cloud Director 데이터베이스로 구성됩니다. 데이터베이스 이름은 vcloud이고 데이터베이스 사용자는 vcloud입니다.</p>

옵션	설명
대기-소	<p>데이터베이스 HA 클러스터의 기본-소 셀에 가입하는 데 사용됩니다.</p> <p>RAM이 12GB이고 vCPU가 2개인 장치를 데이터베이스 고가용성 구성이 있는 VMware Cloud Director 서버 그룹의 두 번째나 세 번째 구성원으로 배포합니다.</p> <p>대기 셀에 내장된 데이터베이스는 복제 모드에서 기본 데이터베이스를 사용하여 구성됩니다.</p>
대기-대	<p>데이터베이스 HA 클러스터의 기본-대 셀에 가입하는 데 사용됩니다.</p> <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 이상 버전은 RAM이 24GB이고 vCPU가 8개인 장치를 데이터베이스 고가용성 구성이 있는 VMware Cloud Director 서버 그룹의 두 번째나 세 번째 구성원으로 배포합니다. ■ VMware Cloud Director 10.2는 RAM이 24GB이고 vCPU가 4개인 장치를 데이터베이스 고가용성 구성이 있는 VMware Cloud Director 서버 그룹의 두 번째나 세 번째 구성원으로 배포합니다. <p>대기 장치에 내장된 데이터베이스는 복제 모드에서 기본 데이터베이스를 사용하여 구성됩니다.</p>
Cloud Director 셀 애플리케이션	<ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 이상 버전은 RAM이 8GB이고 vCPU가 4개인 장치를 VMware Cloud Director 서버 그룹의 후속 구성원으로 배포합니다. ■ VMware Cloud Director 10.2는 RAM이 8GB이고 vCPU가 2개인 장치를 VMware Cloud Director 서버 그룹의 후속 구성원으로 배포합니다. <p>vCD 애플리케이션 셀에 내장된 데이터베이스는 사용되지 않습니다. vCD 애플리케이션 셀이 기본 데이터베이스에 연결됩니다.</p>

중요 VMware Cloud Director 서버 그룹의 기본 셀과 대기 셀은 동일한 크기여야 합니다. 데이터베이스 HA 클러스터는 기본-소 셀 1개와 대기-소 셀 2개로 구성되거나 기본-대 셀 1개와 대기-대 셀 2개로 구성될 수 있습니다.

배포 후에는 장치의 크기를 재구성할 수 있습니다.

- 8 디스크 형식 및 가상 시스템 구성 파일과 가상 디스크의 데이터스토어를 선택하고 **다음**을 클릭합니다.
썸 포맷은 성능을 향상시키고 썸 포맷은 스토리지 공간을 절약합니다.

- 9 **대상 네트워크** 셀의 드롭다운 메뉴에서 장치의 eth1 및 eth0 NIC에 대한 대상 네트워크를 선택합니다.

소스 네트워크 목록이 역순으로 되어 있을 수 있습니다. 각 소스 네트워크에 대해 올바른 대상 네트워크를 선택했는지 확인합니다.

중요 두 대상 네트워크는 서로 달라야 합니다.

- 10 **IP 할당 설정** 드롭다운 메뉴에서 **정적-수동 IP** 할당을 선택하고 **IPv4** 프로토콜을 선택합니다.
- 11 **다음**을 클릭합니다.

VMware Cloud Director 세부 정보를 구성하는 마법사의 **템플릿 사용자 지정** 페이지로 리디렉션됩니다.

12 VCD 장치 설정 섹션에서 장치 세부 정보를 구성합니다.

설정	설명
NTP 서버	사용할 NTP 서버의 호스트 이름 또는 IP 주소입니다.
초기 루트 암호	<p>장치에 대한 초기 루트 암호입니다. 8자 이상이어야 하며 최소한 대문자 1개, 소문자 1개, 숫자 1개 및 특수 문자 1개 사용해야 합니다.</p> <p>중요 초기 루트 암호는 키 저장소 암호가 됩니다. 클러스터를 배포하려면 초기 배포 중에 모든 셀에 동일한 루트 암호가 있어야 합니다. 부팅 프로세스가 끝나면 원하는 셀에서 루트 암호를 변경할 수 있습니다.</p> <p>FIPS 모드를 사용하려면 장치의 루트 암호가 14자 이상이어야 합니다.</p> <p>참고 OVF 배포 마법사는 암호 조건에 대해 초기 루트 암호의 유효성을 검사하지 않습니다.</p>
처음 로그인 시 루트 암호 만료	처음 로그인한 후에 초기 암호를 계속 사용하려면 초기 암호가 루트 암호 조건을 충족하는지 확인해야 합니다. 처음 로그인한 후에 초기 루트 암호를 계속 사용하려면 이 옵션의 선택을 취소합니다.
SSH 루트 로그인 사용	기본적으로 비활성화되어 있습니다.

참고 장치의 날짜, 시간 또는 표준 시간대 변경에 대한 자세한 내용은 <https://kb.vmware.com/kb/59674> 문서를 참조하십시오.

13 (선택 사항) 추가 네트워킹 속성 섹션에서 네트워크 토폴로지에 필요한 경우 eth0 및 eth1 네트워크 인터페이스의 정적 경로를 입력하고 다음을 클릭합니다.

기본이 아닌 게이트웨이 경로를 통해 호스트에 연결하려는 경우 정적 경로를 제공해야 할 수 있습니다. 예를 들어 관리 인프라는 eth1 인터페이스를 통해서만 액세스할 수 있지만 기본 게이트웨이는 eth0에 있습니다. 대부분의 경우 이 설정은 비워 두면 됩니다.

정적 경로는 쉽표로 구분된 경로 규격 목록에 있어야 합니다. 경로 규격은 대상 게이트웨이의 IP 주소와 CIDR(Classless Inter-Domain Routing) 네트워크 규격(선택 사항)으로 구성되어야 합니다. 예: **172.16.100.253 172.16.100.0/19, 172.16.200.253.**

14 네트워킹 속성 섹션에서 eth0 및 eth1 NIC에 대한 네트워크 세부 정보를 입력하고 다음을 클릭합니다.

설정	설명
기본 게이트웨이	장치에 대한 기본 게이트웨이의 IP 주소입니다.
도메인 이름	DNS 검색 도메인입니다(예: <i>mydomain.com</i>).
도메인 검색 경로	<p>장치 호스트 이름 조회를 위해 쉽표 또는 공백으로 구분된 도메인 이름 목록입니다(예: <i>subdomain.example.com</i>).</p> <p>참고 [도메인 이름] 텍스트 상자에 입력한 도메인 이름은 도메인 검색 경로 목록의 첫 번째 요소입니다.</p>
도메인 이름 서버	장치에 대한 도메인 이름 서버의 IP 주소입니다.
eth0 네트워크 IP 주소	eth0 인터페이스의 IP 주소입니다.

설정	설명
eth0 네트워크 넷마스크	eth0 인터페이스의 넷마스크 또는 접두사입니다.
eth1 네트워크 IP 주소	eth1 인터페이스의 IP 주소입니다.
eth1 네트워크 넷마스크	eth1 인터페이스의 넷마스크 또는 접두사입니다.

15 완료 준비 페이지에서 VMware Cloud Director 장치의 구성 설정을 검토한 후 **마침**을 클릭하여 배포를 시작합니다.

다음에 수행할 작업

- 1 새로 만든 가상 시스템의 전원을 켭니다.
- 2 [VMware Cloud Director 기본 장치 구성](#) 또는 [VMware Cloud Director 대기 및 애플리케이션 셀 구성](#) 작업을 수행합니다.

VMware Cloud Director 기본 장치 구성

기본 장치에 대한 OVF 템플릿을 배포한 후에는 기본 VMware Cloud Director 장치 인스턴스의 장치 관리 사용자 인터페이스에서 구성 단계를 계속해야 합니다.

사전 요구 사항

- 1 [VMware Cloud Director 장치 배포 시작](#).
- 2 새로 만든 가상 시스템의 전원을 켭니다.
- 3 [VMware Cloud Director 장치를 위한 전송 서버 스토리지 준비](#) 항목을 숙지합니다.

절차

- 1 웹 브라우저를 열고 `https://Primary-Appliance-eth1-IP-Address:5480`으로 이동합니다.
- 2 기본 장치 인스턴스의 장치 관리 사용자 인터페이스에 로그인합니다.

기본 장치 시스템 설정 페이지가 나타납니다.

- 3 **장치 설정** 섹션에서 장치 세부 정보를 구성하고 **다음**을 클릭합니다.

설정	설명
파일 전송용 NFS 마운트 위치	NFS 공유 전송 서버 스토리지의 위치입니다. VMware Cloud Director는 위치를 검증하고 NFS 마운트가 검증되면 녹색 확인 표시가 나타납니다.
'vcloud' 사용자의 DB 암호	vcloud PostgreSQL 데이터베이스 사용자의 암호입니다.
DB 암호 확인	vcloud PostgreSQL 데이터베이스 사용자의 암호에 대한 확인입니다.
고객 환경 항상 프로그램에 참여	VMware 고객 환경 항상 프로그램에 참여를 활성화하거나 비활성화합니다.

4 관리자 계정 섹션에서 시스템 관리자 세부 정보를 구성하고 다음을 클릭합니다.

설정	설명
사용자 이름	시스템 관리자 계정의 사용자 이름입니다. 기본값은 administrator입니다.
암호	시스템 관리자 계정의 암호입니다. 암호의 길이는 6~128자여야 합니다.
암호 확인	시스템 관리자 계정의 암호를 확인합니다.
전체 이름	시스템 관리자의 전체 이름입니다. 기본값은 vCD Admin입니다.
e-메일 주소	시스템 관리자의 이메일 주소입니다.

5 VMware Cloud Director 설정 섹션에서 이 인스턴스의 설치를 구성합니다.

설정	설명
시스템 이름	VMware Cloud Director 설치를 위해 생성할 vCenter Server 폴더의 이름입니다.
설치 ID	가상 NIC용 MAC 주소를 만들 때 사용할 VMware Cloud Director 설치용 ID 기본값은 1입니다. 다중 사이트 배포에서 VMware Cloud Director 설치 전반에 스트레치된 네트워크를 생성하려는 경우에는 각 VMware Cloud Director 설치에 대해 고유한 설치 ID를 설정하는 것이 좋습니다.

6 제출을 클릭하고 시스템 설정이 완료되면 확인을 클릭합니다.

결과

배포에 성공하면 **내장형 데이터베이스 가용성 및 서비스** 탭이 나타납니다.

다음에 수행할 작업

- [VMware Cloud Director 장치 표준 시간대 변경](#)
- 대기 또는 애플리케이션 셀을 배포합니다. [VMware Cloud Director 장치 배포 시작](#)의 내용을 참조하십시오.
- [VMware Cloud Director 대기 및 애플리케이션 셀 구성](#)

VMware Cloud Director 대기 및 애플리케이션 셀 구성

대기 또는 애플리케이션 셀에 대해 OVF 템플릿을 배포한 후에는 배포하려는 인스턴스의 장치 관리 사용자 인터페이스에서 구성 단계를 계속해야 합니다.

사전 요구 사항

- 1 대기 또는 애플리케이션 셀을 배포합니다. [VMware Cloud Director 장치 배포 시작](#)의 내용을 참조하십시오.
- 2 [VMware Cloud Director 장치를 위한 전송 서버 스토리지 준비](#)의 내용을 참조하십시오.
- 3 새로 만든 가상 시스템의 전원을 켭니다.

절차

- 1 웹 브라우저를 열고 `https://Cell-eth1-IP-Address:5480`으로 이동합니다.
- 2 대기 또는 애플리케이션 셀의 장치 관리 사용자 인터페이스에 로그인합니다.
시스템 설정 페이지가 나타납니다.
- 3 파일 전송용 NFS 마운트 위치를 입력합니다.
- 4 **제출**을 클릭하고 시스템 설정이 완료되면 **확인**을 클릭합니다.

다음에 수행할 작업

VMware Cloud Director 장치 표준 시간대 변경

VMware OVF Tool을 사용하여 VMware Cloud Director 장치 배포

VMware OVF Tool을 사용하여 VMware Cloud Director 장치를 OVF 템플릿으로 배포할 수 있습니다.

VMware Cloud Director 서버 그룹의 첫 번째 구성원을 기본 셀로 배포해야 합니다. VMware Cloud Director 서버 그룹의 후속 구성원은 대기 또는 VMware Cloud Director 애플리케이션 셀로 배포할 수 있습니다. **장치 배포 및 데이터베이스 고가용성 구성**의 내용을 참조하십시오.

OVF Tool 설치에 대한 자세한 내용은 "VMware OVF Tool 릴리스 정보" 문서를 참조하십시오.

OVF Tool 사용에 대한 자세한 내용은 "OVF Tool 사용자 가이드" 를 참조하십시오.

중요 하나의 서버 그룹에서 Linux에 설치된 VMware Cloud Director 및 VMware Cloud Director 장치 배포의 혼합은 지원되지 않습니다.

데이터베이스 클러스터에 추가 또는 교체용 장치를 추가하는 경우 vCPU 및 RAM이 클러스터에 있는 기존의 기본 및 대기 셀과 일치해야 합니다.

새로 배포된 대기 항목의 OVA 버전은 클러스터의 기존 장치와 동일해야 합니다. 실행 중인 장치의 버전을 보려면 장치 관리 UI에서 정보를 참조하십시오. 장치는 VMware Cloud Director-v.v.v.v-
 nnnnnn_OVF10.ova 형식의 이름으로 배포됩니다. 여기서 v.v.v.v는 제품 버전을 나타내고 nnnnnn은 빌드 번호를 나타냅니다. 예: VMware Cloud Director-10.2.0.0-9229800_OVA10.ova.

vSphere에서 OVF 템플릿을 배포하는 방법에 대한 자세한 내용은 "vSphere 가상 시스템 관리" 를 참조하십시오.

아니면 vSphere Client를 사용하여 장치를 배포할 수 있습니다. [vSphere Client를 사용하여 VMware Cloud Director 장치 배포](#)의 내용을 참조하십시오.

배포 명령을 실행하기 전에 [VMware Cloud Director 장치 배포를 위한 사전 요구 사항](#)의 내용을 참조하십시오.

VMware Cloud Director 10.2부터는 VMware Cloud Director 장치를 배포하려면 --

X:enableHiddenProperties 매개 변수를 포함해야 합니다.

참고 기본 장치 배포 중에 선택적 OVF 구성 옵션을 지정할지 아니면 장치 관리 사용자 인터페이스를 실행하여 배포 후에 구성을 완료할지 선택할 수 있습니다.

VMware Cloud Director 장치 배포를 위한 ovftool 명령 옵션 및 속성

옵션	값	설명
--noSSLVerify	해당 없음	vSphere 연결에 대한 SSL 확인을 건너뜁니다.
--acceptAllEulas	해당 없음	모든 EULA(최종 사용자 라이선스 계약)에 동의합니다.
--X:enableHiddenProperties	해당 없음	장치의 구성에 대한 모든 속성을 표시합니다.
--datastore	target_vc_datastore	가상 시스템 구성 파일과 가상 디스크를 저장할 대상 데이터스토어 이름입니다.
--allowAllExtraConfig	해당 없음	모든 추가 구성 옵션을 VMX 형식으로 변환합니다.
--net:"eth0 Network"	portgroup_on_vc_for_eth0	장치 eth0 네트워크의 대상 네트워크입니다. 중요 eth1 대상 네트워크와 달라야 합니다.
--net:"eth1 Network"	portgroup_on_vc_for_eth1	장치 eth1 네트워크의 대상 네트워크입니다. 중요 eth0 대상 네트워크와 달라야 합니다.
--name	vm_name_on_vc	장치의 가상 시스템 이름입니다.
--diskMode	thin 또는 thick	가상 시스템 구성 파일 및 가상 디스크의 디스크 형식입니다.
--prop:"vami.ip0.VMware_vCloud_Director"	eth0_ip_address	eth0의 IP 주소입니다. UI 및 API 액세스에 사용됩니다. 이 주소에서 DNS 역방향 조회는 장치의 호스트 이름을 결정하고 설정합니다.
--prop:"vami.ip1.VMware_vCloud_Director"	eth1_ip_address	eth1의 IP 주소입니다. 내장형 PostgreSQL 데이터베이스 서비스를 비롯한 내부 서비스에 액세스하는 데 사용됩니다.
--prop:"vami.DNS.VMware_vCloud_Director"	dns_ip_address	장치에 대한 도메인 이름 서버의 IP 주소입니다.
--prop:"vami.domain.VMware_vCloud_Director"	domain_name	DNS 검색 도메인입니다. 검색 경로의 첫 번째 요소로 표시됩니다.

옵션	값	설명
--prop:"vami.gateway.VMware_vCloud_Director"	gateway_ip_address	장치에 대한 기본 게이트웨이의 IP 주소입니다.
--prop:"vami.netmask0.VMware_vCloud_Director"	netmask	eth0 인터페이스의 넷마스크 또는 접두사입니다.
--prop:"vami.netmask1.VMware_vCloud_Director"	netmask	eth1 인터페이스의 넷마스크 또는 접두사입니다.
--prop:"vami.searchpath.VMware_vCloud_Director"	directories:domain_names	장치의 도메인 검색 경로입니다. 섬포 또는 공백으로 구분된 도메인 이름 목록입니다.
--prop:"vcloudconf.ceip_enabled.VMware_vCloud_Director"	ceip_enabled	VMware 고객 환경 향상 프로그램에 참여를 활성화하거나 비활성화합니다. 기본값은 true 입니다. 배포 후 장치 관리 사용자 인터페이스를 실행하여 기본 장치 구성을 완료하려는 경우 선택 사항입니다.
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"	enable_ssh	장치에 대한 SSH root 액세스를 활성화하거나 비활성화합니다.
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"	expire_root_password	처음 로그인한 후 초기 암호를 계속 사용할지 여부를 결정합니다.
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"	host_ip_addresses:nfs_mount_path	외부 NFS 서버의 IP 주소 및 내보내기 경로입니다. 기본 셀에만 사용됩니다.
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"	ntp_server_ip_address	시간 서버의 IP 주소입니다.
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"	varoot_password	장치에 대한 초기 루트 암호입니다. 8자 이상이어야 하며 최소한 대문자 1개, 소문자 1개, 숫자 1개 및 특수 문자 1개 사용해야 합니다. 중요 초기 루트 암호는 키 저장소 암호가 됩니다. 클러스터를 배포하려면 초기 배포 중에 모든 셀에 동일한 루트 암호가 있어야 합니다. 부팅 프로세스가 끝나면 원하는 셀에서 루트 암호를 변경할 수 있습니다.
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"	db_password	vcloud 사용자의 데이터베이스 암호입니다. 기본 셀에만 사용됩니다. 배포 후 장치 관리 사용자 인터페이스를 실행하여 기본 장치 구성을 완료하려는 경우 선택 사항입니다.

옵션	값	설명
--prop:"vcloudconf.admin_email.VMware_vCloudDirector_email_address"	vCloudDirector_email_address	시스템 관리자 계정의 이메일 주소입니다. 기본 셀에만 사용됩니다. 배포 후 장치 관리 사용자 인터페이스를 실행하여 기본 장치 구성을 완료하려는 경우 선택 사항입니다.
--prop:"vcloudconf.admin_fname.VMware_vCloudDirector_firstname"	vCloudDirector_firstname	시스템 관리자 계정의 이름입니다. 기본 셀에만 사용됩니다. 배포 후 장치 관리 사용자 인터페이스를 실행하여 기본 장치 구성을 완료하려는 경우 선택 사항입니다.
--prop:"vcloudconf.admin_pwd.VMware_vCloudDirector_password"	vCloudDirector_password	시스템 관리자 계정의 암호입니다. 기본 셀에만 사용됩니다. 배포 후 장치 관리 사용자 인터페이스를 실행하여 기본 장치 구성을 완료하려는 경우 선택 사항입니다.
--prop:"vcloudconf.admin_username.VMware_vCloudDirector_username"	vCloudDirector_username	시스템 관리자 계정의 사용자 이름입니다. 기본 셀에만 사용됩니다. 배포 후 장치 관리 사용자 인터페이스를 실행하여 기본 장치 구성을 완료하려는 경우 선택 사항입니다.
--prop:"vcloudconf.inst_id.VMware_vCloudDirector_ID"	vCloudDirector_ID	VMware Cloud Director 설치 ID입니다. 기본 셀에만 사용됩니다. 배포 후 장치 관리 사용자 인터페이스를 실행하여 기본 장치 구성을 완료하려는 경우 선택 사항입니다.
--prop:"vcloudconf.sys_name.VMware_vCloudSystem_name"	vCloudSystem_name	VMware Cloud Director 설치를 위해 생성할 vCenter Server 폴더의 이름입니다. 배포 후 장치 관리 사용자 인터페이스를 실행하여 기본 장치 구성을 완료하려는 경우 선택 사항입니다.
--prop:"vcloudnet.routes0.VMware_vCloudDirector_ip_addresses" cidr, ip_address2, ...	vCloudDirector_ip_addresses	선택 사항입니다. eth0 인터페이스에 대한 정적 경로입니다. 쉼표로 구분된 경로 규격 목록이어야 합니다. 경로 규격은 게이트웨이의 IP 주소와 CIDR(Classless Inter-Domain Routing) 네트워크 규격(점두사/비트)(선택 사항)으로 구성되어야 합니다. 예: 172.16.100.253 172.16.100/19, 172.16.200.253.

옵션	값	설명
<code>--prop:"vcloudnet.routes1.VMware_vCloud_</code> <code>ip_address1" cidr,</code> <code>ip_address2, ...</code>		<p>선택 사항입니다. eth1 인터페이스에 대한 정적 경로입니다. 쉼표로 구분된 경로 규칙 목록이어야 합니다. 경로 규칙은 게이트웨이의 IP 주소와 CIDR(Classless Inter-Domain Routing) 네트워크 규칙(접두사/비트)(선택 사항)으로 구성되어야 합니다.</p> <p>예:</p> <p>172.16.100.253 172.16.100/19, 172.16.200.253.</p>

옵션	값	설명
--deploymentOption	primary-small, primary-large, standby-small, standby-large 또는 cell	<p>배포하려는 장치 유형 및 크기입니다.</p> <p>기본-소 및 대기-소 VMware Cloud Director 장치 크기는 랩 또는 테스트 시스템에 적합합니다. 기본-대 및 대기-대 크기는 운영 시스템에 대한 최소 크기 조정 요구 사항을 충족합니다. 워크로드에 따라 리소스를 추가해야 할 수도 있습니다.</p> <ul style="list-style-type: none"> ■ primary-small는 RAM이 12GB이고 vCPU가 2개인 장치를 VMware Cloud Director 서버 그룹의 첫 번째 구성원으로 배포합니다. 기본 셀에 내장된 데이터베이스는 VMware Cloud Director 데이터베이스로 구성됩니다. 데이터베이스 이름은 vcloud이고 데이터베이스 사용자는 vcloud입니다. ■ primary-large: <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 이상 버전은 RAM이 24GB이고 vCPU가 8개인 장치를 VMware Cloud Director 서버 그룹의 첫 번째 구성원으로 배포합니다. ■ VMware Cloud Director 10.2는 RAM이 24GB이고 vCPU가 4개인 장치를 VMware Cloud Director 서버 그룹의 첫 번째 구성원으로 배포합니다. <p>기본 셀에 내장된 데이터베이스는 VMware Cloud Director 데이터베이스로 구성됩니다. 데이터베이스 이름은 vcloud이고 데이터베이스 사용자는 vcloud입니다.</p> ■ standby-small는 RAM이 12GB이고 vCPU가 2개인 장치를 데이터베이스 고가용성 구성이 있는 VMware Cloud Director 서버 그룹의 두 번째나 세 번째 구성원으로 배포합니다. 대기 셀에 내장된 데이터베이스는 복제 모드에서 기본 데이터베이스를 사용하여 구성됩니다. ■ standby-large: <ul style="list-style-type: none"> ■ VMware Cloud Director 10.2.1 이상 버전은 RAM이 24GB이고 vCPU가 8개인 장치를 데이터베이스 고가용성 구성이 있는 VMware Cloud Director 서버 그룹의 두 번째나 세 번째 구성원으로 배포합니다.

옵션	값	설명
		<ul style="list-style-type: none"> ■ VMware Cloud Director 10.2는 RAM이 24GB이고 vCPU가 4개인 장치를 데이터베이스 고가용성 구성이 있는 VMware Cloud Director 서버 그룹의 두 번째나 세 번째 구성원으로 배포합니다. <p>대기 셀에 내장된 데이터베이스는 복제 모드에서 기본 데이터베이스를 사용하여 구성됩니다.</p> <ul style="list-style-type: none"> ■ cell: ■ VMware Cloud Director 10.2.1 이상 버전은 RAM이 8GB이고 vCPU가 4개인 장치를 VMware Cloud Director 서버 그룹의 후속 구성원으로 배포합니다. ■ VMware Cloud Director 10.2는 RAM이 8GB이고 vCPU가 2개인 장치를 VMware Cloud Director 서버 그룹의 후속 구성원으로 배포합니다. <p>vCD 애플리케이션 셀에 내장된 데이터베이스는 사용되지 않습니다. vCD 애플리케이션 셀이 기본 데이터베이스에 연결됩니다.</p> <p>중요 VMware Cloud Director 서버 그룹의 기본 셀과 대기 셀은 동일한 크기여야 합니다. 데이터베이스 HA 클러스터는 기본-소 셀 1개와 대기-소 셀 2개로 구성되거나 기본-대 셀 1개와 대기-대 셀 2개로 구성될 수 있습니다.</p> <p>배포 후에는 장치의 크기를 재구성할 수 있습니다.</p>
--powerOn	path_to_ova	배포 후에 가상 시스템 전원을 켭니다.

운영 기본 VMware Cloud Director 장치를 배포하는 명령의 예

중요 VMware OVF Tool 명령을 실행하기 전에 `vcloudapp.varoot-passwordVMware_vCloud_Director`, `vcloudconf.db_pwdVMware_vCloud_Director` 및 `vcloudconf.admin_pwd.VMware_vCloud_Director` 암호를 사용자 자신의 안전한 암호로 바꿉니다.

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--X:enableHiddenProperties \
--datastore='datastore6' \
--allowAllExtraConfig \
```

```
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thick \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-large" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

운영 대기 VMware Cloud Director 장치를 배포하는 명령의 예

중요 VMware OVF Tool 명령을 실행하기 전에 vcloudapp.varoot-password.VMware_vCloud_Director 암호를 사용자 자신의 안전한 암호로 바꿉니다.

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--X:enableHiddenProperties \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thick \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
```

```
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \
--deploymentOption="standby-large" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

VMware Cloud Director 장치 배포 후 작업

장치를 배포한 후에는 firstboot 로그 파일에서 경고 오류 메시지를 확인하십시오. [VMware Cloud Director 장치의 로그 파일 검토](#)의 내용을 참조하십시오.

장치 관리 사용자 인터페이스를 사용하여 기본 장치를 구성합니다. [VMware Cloud Director 기본 장치 구성](#)의 내용을 참조하십시오.

장치 관리 사용자 인터페이스를 사용하여 대기 및 애플리케이션 셀을 구성합니다. [VMware Cloud Director 대기 및 애플리케이션 셀 구성](#)의 내용을 참조하십시오.

HTTPS 및 콘솔 프록시 통신을 위해 서명된 와일드카드 인증서를 사용하여 VMware Cloud Director 장치 배포

서명된 와일드카드 인증서를 사용하여 VMware Cloud Director 장치를 배포할 수 있습니다. 이러한 인증서를 사용하여 인증서에 나열된 도메인 이름의 하위 도메인인 서버를 수 제한 없이 보호할 수 있습니다.

기본적으로 VMware Cloud Director 장치를 배포할 때 VMware Cloud Director는 자체 서명된 인증서를 생성하고 이를 사용하여 HTTPS 및 콘솔 프록시 통신을 위한 VMware Cloud Director 셀을 구성합니다.

기본 장치를 성공적으로 배포하면, 장치 구성 논리가 responses.properties 파일을 기본 장치에서 공통 NFS 공유 전송 서비스 스토리지(/opt/vmware/vcloud-director/data/transfer)로 복사합니다. 이 VMware Cloud Director 서버 그룹에 배포된 다른 장치는 이 파일을 사용하여 자동으로 구성됩니다. responses.properties 파일에는 SSL 인증서 키 저장소에 대한 경로가 포함되어 있습니다. 이 저장소에는 자동 생성된 자체 서명 인증서 user.keystore.path가 포함됩니다. 기본적으로 이 경로는 각 장치의 키 저장소 파일에 대한 로컬 경로입니다.

기본 장치를 배포한 후에 서명된 인증서를 사용하도록 다시 구성할 수 있습니다. 서명된 인증서로 키 저장소를 생성하는 방법에 대한 자세한 내용은 [CA 서명된 SSL 인증서를 생성하고 VMware Cloud Director 장치로 가져오기](#) 항목을 참조하십시오.

기본 VMware Cloud Director 장치에서 사용하는 서명된 인증서가 와일드카드 서명된 인증서인 경우 해당 인증서를 VMware Cloud Director 서버 그룹의 다른 모든 장치(예: 대기 셀 및 VMware Cloud Director 애플리케이션 셀)에 적용할 수 있습니다. HTTPS 및 콘솔 프록시 통신을 위해 서명된 와일드카드 인증서를 통한 장치 배포를 사용하면 서명된 와일드카드 SSL 인증서로 추가 셀을 구성할 수 있습니다.

사전 요구 사항

- HTTPS 및 콘솔 프록시 별칭 모두에 대해 서명된 와일드카드 SSL 인증서를 포함하는 키 저장소를 기본 장치(/opt/vmware/vcloud-director/certificates.ks)에서 사용할 수 있는지 확인합니다.
 - 키 쌍을 만들고 CA 서명된 인증서 파일을 가져오려면 [CA 서명된 SSL 인증서를 생성하고 VMware Cloud Director 장치로 가져오기](#)의 내용을 참조하십시오.
 - 자체 개인 키와 CA 서명된 인증서 파일이 이미 있는 경우 [개인 키 및 CA 서명된 SSL 인증서를 VMware Cloud Director 장치로 가져오기](#)의 내용을 참조하십시오.
- 서명된 와일드카드 SSL 인증서가 포함된 키 저장소의 키 저장소 유형이 JCEKS인 경우 키 저장소 내의 키에 대한 개인 암호가 키 저장소의 암호와 일치하는지 확인해야 합니다. 키 저장소 암호는 모든 장치를 배포할 때 사용되는 초기 루트 암호와 일치해야 합니다.

```
/opt/vmware/vcloud-director/jre/bin/keytool -keypasswd -alias http_or_consoleproxy
-keystore /opt/vmware/vcloud-director/certificates.ks -storetype jceks -storepass root-
password
```

절차

- 1 잘 서명된 인증서가 포함된 새 certificates.ks 파일을 기본 장치에서 전송 공유 위치(/opt/vmware/vcloud-director/data/transfer/)로 복사합니다.

- 2 키 저장소 파일의 소유자 및 그룹 사용 권한을 **vcloud**로 변경합니다.

```
chown vcloud.vcloud /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

- 3 키 저장소 파일의 소유자에게 읽기 및 쓰기 권한이 있는지 확인합니다.

```
chmod 0750 /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

- 4 기본 장치에서 명령을 실행하여 서명된 새 인증서를 VMware Cloud Director 인스턴스로 가져옵니다. 이 명령은 또한 전송 공유의 responses.properties 파일을 업데이트하여 전송 공유의 키 저장소 파일을 가리키도록 *user.keystore.path* 변수를 수정합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
vmware/vcloud-director/data/transfer/certificates.ks --keystore-password root-password
```

- 5 서명된 새 인증서를 적용하려면 기본 장치에서 vmware-vcd 서비스를 다시 시작합니다.

- a 다음 명령을 실행하여 서비스를 중지합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid
cell) -s
```

- b 다음 명령을 실행하여 서비스를 시작합니다.

```
systemctl start vmware-vcd
```

- 6 키 저장소 암호와 일치하는 초기 루트 암호를 사용하여 대기 셀 및 애플리케이션 셀 장치를 배포합니다.

결과

동일한 NFS 공유 전송 서비스 스토리지를 사용하는 새로 배포된 모든 장치는 기본 장치에서 사용하는 동일한 서명된 와일드카드 SSL 인증서로 구성됩니다.

CA 서명된 SSL 인증서를 생성하고 VMware Cloud Director 장치로 가져오기

CA(인증 기관)에서 서명한 인증서를 생성하고 가져오면 SSL 통신에 대해 최고 수준의 신뢰를 제공하고 클라우드는 연결을 보호할 수 있습니다.

각 VMware Cloud Director 서버에는 클라이언트와 서버 간의 통신 보안을 위해 두 개의 SSL 인증서가 필요합니다. 각 VMware Cloud Director 서버는 HTTPS용 및 콘솔 프록시 통신용으로 서로 다른 두 가지 SSL 끝점을 지원해야 합니다.

VMware Cloud Director 장치에서 이러한 두 끝점은 동일한 IP 주소 또는 호스트 이름을 공유하지만 포트는 두 개의 고유한 포트, 즉 HTTPS에는 443, 콘솔 프록시 통신에는 8443을 사용합니다. 끝점마다 고유한 SSL 인증서가 있어야 합니다. 예를 들어 와일드카드 인증서를 사용하여 두 끝점에 동일한 인증서를 사용할 수 있습니다.

두 끝점 모두의 인증서에는 X.500 고유 이름과 X.509 주체 대체 이름 확장이 포함되어야 합니다.

자체 개인 키와 CA 서명 인증서 파일이 이미 있는 경우 [개인 키 및 CA 서명된 SSL 인증서를 VMware Cloud Director 장치로 가져오기](#)에 설명된 절차를 따르십시오.

중요 배포 시 VMware Cloud Director 장치는 키 크기가 2048비트인 자체 서명된 인증서를 생성합니다. 적절한 키 크기를 선택하기 전에 설치의 보안 요구 사항을 평가해야 합니다. 1,024비트보다 작은 키 크기는 NIST Special Publication 800-131A에 따라 더 이상 지원되지 않습니다.

이 절차에서 사용되는 키 저장소 암호는 **root** 사용자 암호이고 이것은 *root_password*로 표시됩니다.

사전 요구 사항

keytool 명령을 숙지합니다. keytool을 사용하여 CA 서명된 SSL 인증서를 VMware Cloud Director 장치로 가져옵니다. VMware Cloud Director는 keytool의 사본을 /opt/vmware/vcloud-director/jre/bin/keytool에 배치합니다.

절차

- 1 VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.

2 환경 요구 사항에 따라 다음 옵션 중 하나를 선택합니다.

VMware Cloud Director 장치를 배포하면 VMware Cloud Director가 HTTPS 서비스 및 콘솔 프록시 서비스에 대해 키 크기가 2048비트인 자체 서명된 인증서를 자동으로 생성합니다.

- CA(인증 기관)를 통해 배포 시 생성된 인증서에 서명하려면 **단계 5단계**로 건너뜁니다.
- 더 큰 키 크기와 같이 사용자 지정 옵션이 포함된 새 인증서를 생성하려면 **단계 3단계**를 계속합니다.

3 명령을 실행하여 기존 certificates.ks 파일을 백업합니다.

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

4 명령을 실행하여 HTTPS 서비스 및 콘솔 프록시 서비스에 대한 공개 및 개인 키 쌍을 생성합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o /opt/vmware/vcloud-director/certificates.ks -w root_password
```

명령은 지정한 암호로 certificates.ks에 키 저장소를 생성하거나 업데이트합니다. 인증서는 명령의 기본값을 사용하여 만들어집니다. 환경의 DNS 구성에 따라 발급자 CN(일반 이름)은 각 서비스의 IP 주소 또는 FQDN으로 설정됩니다. 인증서는 기본 2048비트 키 길이를 사용하고, 만든 지 1년 후에 만료됩니다.

중요 VMware Cloud Director 장치의 구성 제한으로 인해 인증서 키 저장소에 대해 /opt/vmware/vcloud-director/certificates.ks 위치를 사용해야 합니다.

참고 장치 루트 암호를 키 저장소 암호로 사용합니다.

5 HTTPS 서비스 및 콘솔 프록시 서비스에 대한 CSR(인증서 서명 요청)을 생성합니다.

중요 VMware Cloud Director 장치는 HTTPS 서비스와 콘솔 프록시 서비스 모두에 대해 동일한 IP 주소 및 호스트 이름을 공유합니다. 따라서 CSR 생성 명령은 SAN(주체 대체 이름) 확장 인수에 대해 동일한 DNS 및 IP를 포함해야 합니다.

a 인증서 서명 요청을 http.csr 파일에 만듭니다.

```
keytool -keystore certificates.ks -storetype PKCS12 -storepass root_password -certreq -alias http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

b 인증서 서명 요청을 consoleproxy.csr 파일에 만듭니다.

```
keytool -keystore certificates.ks -storetype PKCS12 -storepass root_password -certreq -alias consoleproxy -file consoleproxy.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

6 인증서 서명 요청을 인증 기관에 보냅니다.

인증 기관이 웹 서버 유형을 지정하도록 요구하는 경우 Jakarta Tomcat을 사용합니다.

CA 서명된 인증서를 가져옵니다.

7 CA 서명된 인증서, CA 루트 인증서 및 중간 인증서를 VMware Cloud Director 장치에 복사합니다.**8** 명령을 실행하여 서명된 인증서를 PKCS12 키 저장소로 가져옵니다

- a CA(인증 기관)의 루트 인증서를 root.cer 파일에서 certificates.ks 키 저장소 파일로 가져옵니다.

```
keytool -import -storetype PKCS12 -storepass root_password -keystore /opt/vmware/
vcloud-director/certificates.ks -alias root -file root_certificate_file
```

- b 중간 인증서 파일을 받은 경우 intermediate.cer 파일에서 certificates.ks 키 저장소 파일로 가져옵니다.

```
keytool -import -storetype PKCS12 -storepass root_password -keystore /opt/vmware/
vcloud-director/certificates.ks -alias intermediate -file intermediate_certificate_file
```

- c HTTPS 서비스 인증서를 가져옵니다.

```
keytool -import -storetype PKCS12 -storepass root_password -keystore /opt/vmware/
vcloud-director/certificates.ks -alias http -file http_certificate_file
```

- d 콘솔 프록시 서비스 인증서를 가져옵니다.

```
keytool -import -storetype PKCS12 -storepass root_password -keystore /opt/vmware/
vcloud-director/certificates.ks -alias consoleproxy -file
console_proxy_certificate_file
```

이러한 명령은 certificates.ks 파일을 새로 획득된 CA 서명된 인증서 버전으로 덮어씁니다.

9 인증서를 가져왔는지 확인하려면 명령을 실행하여 키 저장소 파일의 콘텐츠를 나열합니다.

```
keytool -storetype PKCS12 -storepass root_password -keystore /opt/vmware/vcloud-director/
certificates.ks -list
```

10 명령을 실행하여 인증서를 VMware Cloud Director 인스턴스로 가져옵니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
vmware/vcloud-director/certificates.ks --keystore-password root_password
```

- 11 서명된 새 인증서를 적용하려면 VMware Cloud Director 장치에서 `vmware-vcd` 서비스를 다시 시작합니다.

- a 다음 명령을 실행하여 서비스를 중지합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid cell) -s
```

- b 다음 명령을 실행하여 서비스를 시작합니다.

```
systemctl start vmware-vcd
```

다음에 수행할 작업

- 와일드카드 인증서를 사용 중인 경우에는 [HTTPS 및 콘솔 프록시 통신을 위해 서명된 와일드카드 인증서를 사용하여 VMware Cloud Director 장치 배포의 내용을 참조하십시오.](#)
- 와일드카드 인증서를 사용 중이 아니라면 서버 그룹의 모든 VMware Cloud Director 서버에 대해 이 절차를 반복합니다.
- 내장형 PostgreSQL 데이터베이스 및 VMware Cloud Director 장치 관리 사용자 인터페이스의 인증서 교체에 대한 자세한 내용은 [자체 서명된 내장형 PostgreSQL 및 VMware Cloud Director 장치 관리 UI 인증서 교체 항목을 참조하십시오.](#)

개인 키 및 CA 서명된 SSL 인증서를 VMware Cloud Director 장치로 가져오기

자체 개인 키 및 CA 서명 인증서 파일이 있는 경우 VMware Cloud Director 환경에 키 저장소를 가져오기 전에 HTTPS와 콘솔 프록시 서비스 모두에 대한 인증서 및 개인 키를 가져올 키 저장소 파일을 생성해야 합니다.

사전 요구 사항

- `keytool` 명령을 숙지합니다. `keytool`을 사용하여 CA 서명된 SSL 인증서를 VMware Cloud Director 장치로 가져옵니다. VMware Cloud Director는 `keytool`의 사본을 `/opt/vmware/vcloud-director/jre/bin/keytool`에 배치합니다.
- 중간 인증서, 루트 CA 인증서, CA 서명된 HTTPS 서비스 및 콘솔 프록시 서비스 개인 키 및 인증서를 장치에 복사합니다.

절차

- 1 VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 중간 인증서가 있는 경우 명령을 실행하여 루트 CA 서명 인증서를 중간 인증서와 결합하고 인증서 체인을 생성합니다.

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```

- 3 OpenSSL을 사용하여 개인 키, 인증서 체인 및 해당 별칭으로 HTTPS와 콘솔 프록시 서비스 모두에 대한 중간 키 저장소 파일을 생성하고 각 키 저장소 파일에 대한 암호를 지정합니다.

- a HTTPS 서비스에 대한 키 저장소 파일을 생성합니다.

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http
-passout pass:keystore_password -out http.p12 -chain
```

- b 콘솔 프록시 서비스에 대한 키 저장소 파일을 생성합니다.

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt
-name consoleproxy -passout pass:keystore_password -out consoleproxy.p12 -chain
```

- 4 명령을 실행하여 기존 certificates.ks 파일을 백업합니다.

```
cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
```

- 5 keytool 명령을 사용하여 PKCS12 키 저장소를 certificates.ks 키 저장소로 가져옵니다.

- a HTTPS 서비스에 대한 PKCS12 키 저장소를 가져옵니다.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/
vcloud-director/certificates.ks -deststoretype PKCS12 -srckeystore http.p12
-srcstoretype PKCS12 -srcstorepass keystore_password
```

- b 콘솔 프록시 서비스에 대한 PKCS12 키 저장소를 가져옵니다.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/
vcloud-director/certificates.ks -deststoretype PKCS12 -srckeystore consoleproxy.p12
-srcstoretype PKCS12 -srcstorepass keystore_password
```

- 6 인증서 가져오기가 성공했는지 확인합니다.

```
keytool -storetype PKCS12 -storepass keystore_password -keystore /opt/vmware/vcloud-
director/certificates.ks -list
```

- 7 명령을 실행하여 서명된 인증서를 VMware Cloud Director 인스턴스로 가져옵니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
vmware/vcloud-director/certificates.ks --keystore-password keystore_password
```

- 8 CA 서명된 인증서를 적용하려면 VMware Cloud Director 장치에서 vmware-vcd 서비스를 다시 시작합니다.

```
service vmware-vcd restart
```

다음에 수행할 작업

- 와일드카드 인증서를 사용 중인 경우에는 HTTPS 및 콘솔 프록시 통신을 위해 서명된 와일드카드 인증서를 사용하여 VMware Cloud Director 장치 배포의 내용을 참조하십시오.

- 와일드카드 인증서를 사용 중이 아니라면 서버 그룹의 모든 VMware Cloud Director 장치 셀에 대해 이 절차를 반복합니다.
- 내장형 PostgreSQL 데이터베이스 및 VMware Cloud Director 장치 관리 사용자 인터페이스의 인증서 교체에 대한 자세한 내용은 [자체 서명된 내장형 PostgreSQL 및 VMware Cloud Director 장치 관리 UI 인증서 교체](#) 항목을 참조하십시오.

VMware Cloud Director 장치 배포 후 작업

VMware Cloud Director 서버 그룹을 생성한 후에는 Microsoft Sysprep 파일 및 Cassandra 데이터베이스를 설치할 수 있습니다. PostgreSQL 데이터베이스를 사용하는 경우에는 데이터베이스에서 SSL을 구성하고 일부 매개 변수를 조정할 수 있습니다.

VMware Cloud Director 장치를 생성한 후 vSphere 네트워킹 기능을 사용하여 새 NIC(네트워크 인터페이스 카드)를 추가할 수 있습니다. "vSphere 가상 시스템 관리" 가이드에서 [가상 시스템에 네트워크 어댑터 추가](#) 정보를 참조하십시오.

참고 클러스터가 자동 페일오버에 대해 구성되어 있다면 하나 이상의 추가 셀을 배포한 후 장치 API를 사용하여 클러스터 페일오버 모드를 Automatic으로 재설정해야 합니다. [VMware Cloud Director 장치 API](#)를 참조하십시오. 새 셀에 대한 기본 페일오버 모드는 Manual입니다. 클러스터의 노드 전체에서 페일오버 모드가 일관되지 않은 경우 클러스터 페일오버 모드는 Indeterminate입니다. Indeterminate 모드는 이전 기본 셀 이후 노드와 기타 노드 간에 일관성 없는 클러스터 상태를 초래할 수 있습니다. 클러스터 페일오버 모드를 보려면 [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.

버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)의 내용을 참조하십시오.

VMware Cloud Director 장치 표준 시간대 변경

VMware Cloud Director 장치를 성공적으로 배포한 후 장치의 시스템 표준 시간대를 변경할 수 있습니다. 전송 서버 스토리지 및 서버 그룹의 모든 VMware Cloud Director 장치 인스턴스는 동일한 설정을 사용해야 합니다.

사전 요구 사항

- VMware Cloud Director 장치를 배포합니다. [VMware Cloud Director 장치의 배포 및 초기 구성](#)의 내용을 참조하십시오.
- 전송 서버 스토리지 표준 시간대를 VMware Cloud Director 기본 장치의 새 표준 시간대로 변경합니다.

절차

- 1 기본 노트에 대한 웹 콘솔 또는 원격 콘솔을 사용하여 콘솔 창의 왼쪽 아래에서 **표준 시간대 설정**을 선택합니다.
- 2 위치, 국가 및 표준 시간대 지역을 선택합니다.
새로 선택한 표준 시간대가 콘솔 창의 왼쪽 아래에 나타납니다.
- 3 VMware Cloud Director 장치 콘솔에 **루트**로 로그인합니다.
- 4 VMware Cloud Director 장치에 새로운 표준 시간대가 사용되도록 하려면 `vmware-vcd` 서비스를 다시 시작합니다.
- 5 VMware Cloud Director 배포의 모든 대기 및 애플리케이션 셀에 대해 1단계에서 단계 4단계를 반복합니다.

VMware Cloud Director 장치의 공개 주소 사용자 지정

로드 밸런서 또는 프록시 요구 사항을 충족하기 위해 VMware Cloud Director 웹 포털, VMware Cloud Director API 및 콘솔 프록시에 대한 기본 끝점 웹 주소를 변경할 수 있습니다.

장치가 콘솔 프록시 서비스에 대해 사용자 지정 포트 8443이 포함된 단일 IP 주소를 사용하기 때문에 VMware Cloud Director 공용 콘솔 프록시 주소를 구성해야 합니다. 6의 내용을 참조하십시오.

사전 요구 사항

시스템 관리자로 로그인했는지 확인합니다. **시스템 관리자**만 공용 끝점을 사용자 지정할 수 있습니다.

절차

- 1 Service Provider Admin Portal의 위쪽 탐색 모음에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **설정** 아래에서 **공개 주소**를 클릭합니다.
- 3 공용 끝점을 사용자 지정하려면 **편집**을 클릭합니다.
- 4 VMware Cloud Director URL을 사용자 지정하려면 **웹 포털** 끝점을 편집합니다.
 - a HTTPS(보안) 연결을 위한 사용자 지정 VMware Cloud Director 공용 URL을 입력하고 **업로드**를 클릭하여 해당 끝점의 신뢰 체인을 설정하는 인증서를 업로드합니다.

인증서 체인은 서비스 끝점에서 사용되는 인증서와 일치해야 하며, 이것은 별칭이 `consoleproxy`인 각 VMware Cloud Director 셀 키 저장소에 업로드된 인증서입니다. 로드 밸런서에서 콘솔 프록시 연결의 SSL 종료는 지원되지 않습니다. 인증서 체인에는 끝점 인증서, 중간 인증서 및 개인 키 없는 PEM 형식의 루트 인증서가 포함되어야 합니다.

5 (선택 사항) Cloud Director REST API와 OpenAPI URL을 사용자 지정하려면 웹 포털 설정 사용 토글을 해제합니다.

a 사용자 지정 HTTP 기본 URL을 입력합니다.

예를 들어 HTTP 기본 URL을 **http://vcloud.example.com**으로 설정하면 `http://vcloud.example.com/api`에서 VMware Cloud Director API에 액세스하고 `http://vcloud.example.com/cloudapi`에서 VMware Cloud Director OpenAPI에 액세스할 수 있습니다.

b 사용자 지정 HTTPS REST API 기본 URL을 입력하고 업로드를 클릭하여 해당 끝점의 신뢰 체인을 설정하는 인증서를 업로드합니다.

예를 들어 HTTPS REST API 기본 URL을 **https://vcloud.example.com**으로 설정하면 `https://vcloud.example.com/api`에서 VMware Cloud Director API에 액세스하고 `https://vcloud.example.com/cloudapi`에서 VMware Cloud Director OpenAPI에 액세스할 수 있습니다.

인증서 체인은 서비스 끝점에 사용되는 인증서와 일치해야 하며, 별칭이 http인 각 VMware Cloud Director 셀 키 저장소에 업로드된 인증서이거나 SSL 종료가 사용되는 경우 로드 밸런서 VIP 인증서입니다. 인증서 체인에는 끝점 인증서, 중간 인증서 및 개인 키 없는 PEM 형식의 루트 인증서가 포함되어야 합니다.

6 사용자 지정 VMware Cloud Director 공용 콘솔 프록시 주소를 입력합니다.

이 주소는 VMware Cloud Director 장치 eth0 NIC의 FQDN(정규화된 도메인 이름)으로, FQDN 또는 IP 주소로 지정되고 콘솔 프록시 서비스를 위한 사용자 지정 포트 **8443**이 포함됩니다.

예를 들어 FQDN이 `vcloud.example.com`인 VMware Cloud Director 장치 인스턴스의 경우 **vcloud.example.com:8443**을 입력합니다.

VMware Cloud Director는 VM에서 원격 콘솔 창을 열 때 콘솔 프록시 주소를 사용합니다.

7 변경 내용을 저장하려면 저장을 클릭합니다.

기간별 메트릭 데이터 저장을 위한 Cassandra 데이터베이스 설치 및 구성

VMware Cloud Director는 클라우드에 있는 가상 시스템의 가상 시스템 성능 및 리소스 사용에 대한 현재 및 이전 정보를 제공하는 메트릭을 수집할 수 있습니다. 이전 메트릭에 대한 데이터는 Cassandra 클러스터에 저장됩니다.

Cassandra는 오픈 소스 데이터베이스로, 가상 시스템 메트릭과 같은 시계열 데이터를 수집하는 확장 가능한 고성능 솔루션용 백업 저장소를 제공하는 데 사용할 수 있습니다. VMware Cloud Director에서 가상 시스템의 이전 메트릭 검색을 지원하도록 하려면 Cassandra 클러스터를 설치 및 구성하고 `cell-management-tool`을 사용하여 클러스터를 VMware Cloud Director에 연결해야 합니다. 현재 메트릭을 검색할 경우에는 데이터베이스 소프트웨어(선택 사항)가 필요하지 않습니다.

사전 요구 사항

- 데이터베이스 소프트웨어(선택 사항)를 구성하기 전에 VMware Cloud Director가 설치되어 실행 중인지 확인합니다.
- Cassandra에 아직 익숙하지 않은 경우 <http://cassandra.apache.org/>에서 자료를 검토합니다.
- 메트릭 데이터베이스로 사용하기 위해 지원되는 Cassandra 릴리스 목록은 "VMware Cloud Director 릴리스 정보" 항목을 참조하십시오. <http://cassandra.apache.org/download/>에서 Cassandra를 다운로드할 수 있습니다.
- Cassandra 클러스터 설치 및 구성:
 - Cassandra 클러스터에는 2개 이상의 호스트에 배포된 4개 이상의 가상 시스템이 포함되어야 합니다.
 - 2개의 Cassandra 시드 노드가 필요합니다.
 - Cassandra 클라이언트와 노드 간 암호화를 사용하도록 설정합니다. <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html>의 내용을 참조하십시오.
 - Cassandra 사용자 인증을 사용하도록 설정합니다. <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html>의 내용을 참조하십시오.
 - 각 Cassandra 클러스터에서 JNA(Java Native Access) 버전 3.2.7 이상을 사용하도록 설정합니다.
 - Cassandra 노드 간 암호화는 선택 사항입니다.
 - Cassandra에서 SSL의 사용은 선택 사항입니다. Cassandra에 대한 SSL을 사용하도록 설정하지 않는 경우 각 셀(\$VCLOUD_HOME/etc/global.properties)의 global.properties 파일에서 구성 매개 변수 `cassandra.use.ssl`을 0으로 설정해야 합니다.

절차

- 1 cell-management-tool 유틸리티를 사용하여 VMware Cloud Director와 Cassandra 클러스터의 노드 간에 연결을 구성합니다.

다음 명령 예에서 *node1-ip*, *node2-ip*, *node3-ip* 및 *node4-ip*는 Cassandra 클러스터 구성원의 IP 주소입니다. 기본 포트(9042)가 사용됩니다. 메트릭 데이터는 15일 동안 유지됩니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
```

셀 관리 도구를 사용하는 방법에 대한 정보는 [장 5 셀 관리 도구 참조 사항](#)의 내용을 참조하십시오.

- 2 (선택 사항) VMware Cloud Director를 버전 9.1에서 업그레이드하는 경우 `cell-management-tool`을 사용하여 메트릭 데이터베이스가 롤업된 메트릭을 저장하도록 구성합니다.

다음 예와 유사한 명령을 실행합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password
'P@55w0rd'
```

- 3 각 VMware Cloud Director 셀을 다시 시작합니다.

RabbitMQ AMQP 브로커 설치 및 구성

차단 작업, 알림 또는 VMware Cloud Director API 확장(예: Container Service Extension (CSE) 또는 VMware Cloud Director App Launchpad)을 사용하려면 RabbitMQ AMQP 브로커를 설치하고 구성해야 합니다.

AMQP(Advanced Message Queuing Protocol)는 기업 시스템에 유연한 메시징을 지원하는 메시지 대기열 기능의 개방형 표준입니다. VMware Cloud Director는 확장 서비스, 개체 확장 및 알림에 사용되는 메시지 버스를 제공하기 위해 RabbitMQ AMQP 브로커를 사용합니다.

VMware Cloud Director의 경우, 알림을 구성할 때 RabbitMQ AMQP 브로커 대신 MQTT 클라이언트를 사용할 수 있습니다. [MQTT 클라이언트를 사용하여 이벤트, 작업 및 메트릭 구독의 내용을 참조하십시오.](#)

절차

- 1 <https://www.rabbitmq.com/download.html>에서 RabbitMQ Server를 다운로드합니다.
지원되는 RabbitMQ 릴리스의 목록을 보려면 "VMware Cloud Director 릴리스 정보"를 참조하십시오.
- 2 RabbitMQ 설치 지침에 따라 RabbitMQ를 지원되는 호스트에 설치합니다.
각 VMware Cloud Director 셀에서 네트워크에 있는 RabbitMQ 서버 호스트에 액세스할 수 있어야 합니다.
- 3 RabbitMQ를 설치하는 동안 이 RabbitMQ 설치 환경과 연동하도록 VMware Cloud Director를 구성하는 데 필요한 값을 기록해 둡니다.
 - RabbitMQ 서버 호스트의 정규화된 도메인 이름(예: *amqp.example.com*)
 - RabbitMQ를 인증하는 데 유효한 사용자 이름과 암호
 - 브로커가 메시지를 수신하는 포트입니다. 기본값은 비SSL의 경우 5672입니다. SSL/TLS에 대한 기본 포트는 5671입니다.
 - 통신 프로토콜은 TCP입니다.
 - RabbitMQ 가상 호스트입니다. 기본값은 "/"입니다.

다음에 수행할 작업

기본적으로 VMware Cloud Director AMQP 서비스는 암호화되지 않은 메시지를 보냅니다. SSL을 사용하여 이러한 메시지를 암호화하도록 AMQP 서비스를 구성할 수 있습니다. VMware Cloud Director 셀에 있는(일반적인 위치: \$VCLLOUD_HOME/jre/lib/security/cacerts) Java Runtime Environment의 기본 JCEKS 신뢰 저장소를 사용하여 브로커 인증서를 확인하도록 서비스를 구성할 수도 있습니다.

VMware Cloud Director AMQP 서비스에서 SSL을 사용하도록 설정하려면 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 [AMQP 브로커 구성](#) 정보를 참조하십시오.

VMware Cloud Director 장치 루트 암호 변경

VMware Cloud Director 장치의 루트 암호를 변경하면 새 암호를 사용하도록 장치 인증서 키 저장소도 업데이트해야 합니다.

사전 요구 사항

- `keytool` 명령을 숙지합니다. VMware Cloud Director는 `keytool`의 사본을 `/opt/vmware/vcloud-director/jre/bin/keytool`에 배치합니다.
- 와일드카드 인증서를 사용하고 있으며 이 인증서를 NFS 공유 전송 스토리지에 저장하는 경우 인증서가 업데이트되었는지 확인하려면 [HTTPS](#) 및 콘솔 프록시 통신을 위해 서명된 와일드카드 인증서를 사용하여 [VMware Cloud Director](#) 장치 배포에 설명된 절차를 따르십시오.

절차

- 1 VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 `passwd` 명령을 실행하고 **루트** 사용자의 암호를 변경합니다.

```
passwd root
```

참고 FIPS 모드를 사용하도록 설정한 경우 장치의 **루트** 암호는 14자 이상을 포함해야 합니다.

참고 루트 암호가 이미 만료된 경우 VMware Cloud Director는 VMware Cloud Director 장치 콘솔에 **루트**로 처음 로그인할 때 암호를 설정하라는 메시지를 표시합니다.

- 3 명령을 실행하여 기존 인증서 키 저장소 파일을 백업합니다.

```
cp /opt/vmware/vcloud-director/certificates.ks /tmp/certificates.ks
```

- 4 새 인증서 키 저장소를 생성하려면 `keytool` 명령을 실행합니다.

```
keytool -importkeystore -srckeystore /opt/vmware/vcloud-director/certificates.ks
-srcstoretype PKCS12 -srcstorepass old_root_password -destkeystore /opt/vmware/vcloud-
director/certificates-new.ks -deststoretype PKCS12 -deststorepass new_root_password
-destkeypass new_root_password
```

참고 VMware Cloud Director 10.2부터 VMware Cloud Director 장치의 기본 인증서 키 저장소 유형은 PKCS12입니다. 버전 10.2로 업그레이드된 장치 버전을 사용하는 경우에는 JCEKS를 `-srcstoretype` 및 `-deststoretype`으로 사용합니다.

```
keytool -importkeystore -srckeystore /opt/vmware/vcloud-director/certificates.ks
-srcstoretype JCEKS -srcstorepass old_root_password -destkeystore /opt/vmware/vcloud-
director/certificates-new.ks -deststoretype JCEKS -deststorepass new_root_password
-destkeypass new_root_password
```

- 5 명령을 실행하여 이전 인증서 키 저장소 파일을 새 파일로 바꿉니다.

```
mv /opt/vmware/vcloud-director/certificates-new.ks /opt/vmware/vcloud-director/
certificates.ks
```

- 6 키 저장소 파일의 사용자 및 그룹 소유권을 확인하려면 `chown` 명령을 실행합니다.

```
chown vcloud.vcloud /opt/vmware/vcloud-director/certificates.ks
```

- 7 키 저장소의 새 암호를 사용하려면 VMware Cloud Director 서버 구성을 업데이트합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
vmware/vcloud-director/certificates.ks --keystore-password new_root_password
```

다음에 수행할 작업

클러스터의 각 장치에서 이 절차를 반복합니다.

중요 모든 장치는 동일한 루트 암호를 공유해야 합니다. 새로 배포된 장치는 새 루트 암호를 사용해야 합니다.

VMware Cloud Director 장치 업그레이드 및 마이그레이션

버전 9.7부터는 VMware Cloud Director 장치에고가용성 기능이 있는 내장형 PostgreSQL 데이터베이스가 포함됩니다. VMware Cloud Director 장치를 이후 버전으로 업그레이드할 수 있습니다. 외부 PostgreSQL 데이터베이스를 사용하는 이전 버전의 기존 VMware Cloud Director를 VMware Cloud Director 장치 배포 버전 10.0 이상으로 구성된 VMware Cloud Director 환경으로 마이그레이션할 수 있습니다.

VMware Cloud Director 장치 업그레이드

VMware Cloud Director 장치 버전 9.7을 버전 10.2로 업그레이드하려면 [업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드](#)의 내용을 참조하십시오.

VMware Cloud Director 10.0부터 Microsoft SQL Server 데이터베이스가 지원되지 않습니다.

VMware Cloud Director를 업그레이드 하는 경우 새 버전이 기존 설치의 다음 구성 요소와 호환되어야 합니다.

- VMware Cloud Director 데이터베이스에 현재 사용 중인 데이터베이스 소프트웨어. 자세한 내용은 업그레이드 및 마이그레이션 경로 테이블을 참조하십시오.
- 현재 사용 중인 VMware vSphere® 릴리스입니다.
- 현재 사용 중인 VMware NSX® 릴리스입니다.
- VMware Cloud Director와 직접 상호 작용하는 모든 타사 구성 요소.

VMware Cloud Director와 다른 VMware 제품 및 타사 데이터베이스와의 호환성에 대한 정보는 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php에서 "VMware 제품 상호 운용성 매트릭스"를 참조하십시오. VMware Cloud Director 업그레이드의 일환으로 vSphere 또는 NSX 구성 요소를 업그레이드하려면 VMware Cloud Director를 업그레이드한 후에 업그레이드해야 합니다. [VMware Cloud Director 업그레이드 후 작업](#)의 내용을 참조하십시오.

하나 이상의 VMware Cloud Director 서버를 업그레이드한 후에 VMware Cloud Director 데이터베이스를 업그레이드할 수 있습니다. 데이터베이스는 실행 중인 모든 VMware Cloud Director 작업의 상태를 비롯한 서버의 런타임 상태에 대한 정보를 저장합니다. 업그레이드 후 잘못된 작업 정보가 데이터베이스에 남아 있지 않도록 하려면 업그레이드를 시작하기 전에 모든 서버에서 활성 상태의 작업이 없는지를 확인해야 합니다.

또한 VMware Cloud Director 데이터베이스에 저장되지 않은 다음의 아티팩트도 업그레이드할 때 유지됩니다.

- 로컬 및 전역 속성 파일은 새 설치 환경에 복사됩니다.
- 게스트 사용자 지정 지원에 사용되는 Microsoft Sysprep 파일은 새 설치 환경에 복사됩니다.

이 업그레이드에는 서버 그룹 및 데이터베이스의 모든 서버를 업그레이드하기에 충분한 VMware Cloud Director 다운타임이 필요합니다. 로드 밸런서를 사용하는 경우 메시지(예: 시스템이 업그레이드를 위해 오프라인 상태입니다.)를 반환하도록 로드 밸런서를 구성할 수 있습니다.

버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)의 내용을 참조하십시오.

중요 버전 10.1 이상으로 업그레이드한 후 VMware Cloud Director는 연결된 모든 인프라 끝점에 대한 인증서를 항상 확인합니다. 이는 VMware Cloud Director가 SSL 인증서를 관리하는 방식이 변경되었기 때문입니다. 업그레이드 전에 인증서를 VMware Cloud Director로 가져오지 않으면 SSL 확인 문제로 인해 vCenter Server 및 NSX 연결에 실패한 연결 오류가 표시될 수 있습니다. 이 경우 업그레이드 후 다음 두 가지 옵션이 제공됩니다.

- 1 셸 관리 도구 `trust-infra-certs` 명령을 실행하여 모든 인증서를 중앙 집중식 인증서 저장소로 자동으로 가져옵니다. [vSphere 리소스에서 끝점 인증서 가져오기](#)를 참조하십시오.
- 2 Service Provider Admin Portal UI에서 각 vCenter Server 및 NSX 인스턴스를 선택하고 인증서를 수락하는 동안 자격 증명을 다시 입력합니다.

VMware Cloud Director 장치 마이그레이션

기존 VMware Cloud Director 서버 그룹이 VMware Cloud Director 9.5 장치 배포로 구성된 경우 환경을 보다 최신 버전의 VMware Cloud Director 장치로만 마이그레이션할 수 있습니다. Linux용 VMware Cloud Director 설치 관리자를 사용하여 마이그레이션 워크플로의 일부로만 기존 환경을 업그레이드합니다. [vCloud Director 장치로 마이그레이션](#)을 참조하십시오.

VMware Cloud Director 환경에서 외부 Oracle 데이터베이스나 외부 Microsoft SQL 데이터베이스를 사용하는 경우에는 VMware Cloud Director 10.2로 업그레이드하기 전에 PostgreSQL 데이터베이스로 마이그레이션해야 합니다. 업그레이드 경로는 [Linux에서 VMware Cloud Director 업그레이드](#)의 내용을 참조하십시오.

업그레이드 및 마이그레이션 경로 및 워크플로

소스 환경	대상 환경	
	내장형 PostgreSQL 데이터베이스를 사용하는 VMware Cloud Director 장치 10.2	
외부 Microsoft SQL Server 데이터베이스를 사용하는 Linux의 VMware Cloud Director 9.7	1	VMware Cloud Director 장치 9.7로 마이그레이션합니다. 외부 Microsoft SQL 데이터베이스를 사용하여 vCloud Director를 vCloud Director 장치에 마이그레이션을 참조하십시오.
	2	환경을 VMware Cloud Director 장치 10.2로 업그레이드합니다. 업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드의 내용을 참조하십시오.
외부 PostgreSQL 데이터베이스를 사용하는 Linux의 VMware Cloud Director 9.7	1	VMware Cloud Director 장치 9.7로 마이그레이션합니다. 외부 PostgreSQL 데이터베이스를 사용하여 vCloud Director를 vCloud Director 장치에 마이그레이션을 참조하십시오.
	2	환경을 VMware Cloud Director 장치 10.2로 업그레이드합니다. 업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드의 내용을 참조하십시오.
외부 PostgreSQL 데이터베이스를 사용하는 Linux의 VMware Cloud Director 10.0	1	VMware Cloud Director 장치 10.0으로 마이그레이션합니다. 외부 PostgreSQL 데이터베이스를 사용하는 vCloud Director를 vCloud Director 장치에 마이그레이션을 참조하십시오.
	2	환경을 VMware Cloud Director 장치 10.2로 업그레이드합니다. 업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드의 내용을 참조하십시오.
외부 PostgreSQL 데이터베이스를 사용하는 Linux의 VMware Cloud Director 10.1	1	VMware Cloud Director 장치 10.1로 마이그레이션합니다. 외부 PostgreSQL 데이터베이스를 사용하는 VMware Cloud Director를 VMware Cloud Director 장치에 마이그레이션을 참조하십시오.
	2	환경을 VMware Cloud Director 장치 10.2로 업그레이드합니다. 업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드의 내용을 참조하십시오.
내장형 PostgreSQL 데이터베이스를 사용하는 VMware Cloud Director 장치 9.7, 10.0 또는 10.1	환경을 VMware Cloud Director 장치 10.2로 업그레이드합니다. 업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드의 내용을 참조하십시오.	

업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드

업데이트 패키지를 사용하여 VMware Cloud Director 장치를 최신 버전으로 업그레이드하거나 VMware Cloud Director 장치에 패치를 적용할 수 있습니다.

VMware Cloud Director 장치 배포를 업그레이드하는 동안 VMware Cloud Director 서비스가 작동을 중지하고 다운타임이 발생할 수 있습니다. 다운타임은 각 VMware Cloud Director 장치를 업그레이드하고 VMware Cloud Director 데이터베이스 업그레이드 스크립트를 실행하는 데 필요한 시간에 따라 달라집니다. VMware Cloud Director 서버 그룹의 작업 셀 수는 마지막 VMware Cloud Director 장치에서 VMware Cloud Director 서비스를 중지할 때까지 줄어듭니다. VMware Cloud Director HTTP 끝점 앞에 올바르게 구성된 로드 밸런서는 중지된 셀에 대한 트래픽 라우팅을 중지해야 합니다.

모든 VMware Cloud Director 장치에 업그레이드를 적용하고 데이터베이스 업그레이드가 완료된 후에는 각각의 VMware Cloud Director 장치를 재부팅해야 합니다.

사전 요구 사항

기본 VMware Cloud Director 장치의 스냅샷을 생성합니다.

- 1 버전 10.1 이상에서 업그레이드하거나 패치를 적용할 때 기본 데이터베이스 서비스 장애가 발생하는 경우 자동 페일오버를 사용하도록 설정하는 경우, 업그레이드 중에 페일오버 모드를 Manual로 변경합니다. 업그레이드 후에는 페일오버 모드를 Automatic으로 설정할 수 있습니다. [VMware Cloud Director 장치의 자동 페일오버](#)의 내용을 참조하십시오.
- 2 데이터베이스 고가용성 클러스터의 기본 VMware Cloud Director 장치가 있는 vCenter Server 인스턴스에 로그인합니다.
- 3 기본 VMware Cloud Director 장치로 이동하여 해당 장치를 마우스 오른쪽 버튼으로 클릭한 다음 **전원 > 게스트 OS 종료**를 클릭합니다.
- 4 장치를 마우스 오른쪽 버튼으로 클릭하고 **스냅샷 > 스냅샷 생성**을 클릭합니다. 스냅샷의 이름과 설명(선택 사항)을 입력하고 **확인**을 클릭합니다.
- 5 VMware Cloud Director 장치를 마우스 오른쪽 버튼으로 클릭하고 **전원 > 전원 켜기**를 클릭합니다.
- 6 데이터베이스 고가용성 구성의 모든 노드가 정상 상태인지 확인합니다. [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.

절차

- 1 웹 브라우저에서 VMware Cloud Director 장치 인스턴스의 장치 관리 사용자 인터페이스에 로그인하여 기본 장치를 식별합니다(https://appliance_ip_address:5480).

기본 장치 이름을 기록해 둡니다. 대기 및 애플리케이션 셀 보다 먼저 기본 장치를 업그레이드해야 합니다. 데이터베이스를 백업할 때는 기본 장치를 사용해야 합니다.

- 2 업그레이드 중인 장치에 업데이트 패키지를 다운로드합니다.

참고 먼저 기본 장치를 업그레이드해야 합니다.

VMware Cloud Director는 이름이 `VMware_Cloud_Director_v.v.v.v-
nnnnnnnnn_update.tar.gz` 형식인 실행 파일로 배포되며, 여기서 `v.v.v.v`는 제품 버전을 나타내고 `nnnnnnnnn`은 빌드 번호를 나타냅니다. 예:

`VMware_Cloud_Director_10.1.0.4424-14420378_update.tar.gz`.

- 3 업데이트 패키지를 추출할 local-update-package 디렉토리를 생성합니다.

```
mkdir /tmp/local-update-package
```

- 4 새로 생성한 디렉토리에 업데이트 패키지를 추출합니다.

```
tar -zxf VMware_Cloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz \
-C /tmp/local-update-package
```

- 5 local-update-package 디렉토리를 업데이트 저장소로 설정합니다.

```
vamicli update --repo file:///tmp/local-update-package
```

- 6 업데이트를 확인하여 저장소를 올바르게 설정했는지 확인합니다.

```
vamicli update --check
```

업그레이드 릴리스가 사용 가능한 업데이트로 표시됩니다.

- 7 다음 명령을 실행하여 VMware Cloud Director를 종료합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 8 사용 가능한 업그레이드를 적용합니다.

```
vamicli update --install latest
```

- 9 나머지 대기 및 애플리케이션 셀에서 2~8을 반복합니다.

- 10 기본 장치에서 VMware Cloud Director 장치에 내장된 데이터베이스를 백업합니다.

```
/opt/vmware/appliance/bin/create-db-backup
```

- 11 임의 장치에서 VMware Cloud Director 데이터베이스 upgrade 유틸리티를 실행합니다.

```
/opt/vmware/vcloud-director/bin/upgrade
```

- 12 각 VMware Cloud Director 장치를 재부팅합니다.

```
shutdown -r now
```

다음에 수행할 작업

- 업그레이드에 성공하면 VMware Cloud Director 장치의 스냅샷을 삭제할 수 있습니다.
- 업그레이드에 성공하지 못하면 VMware Cloud Director 장치를 업그레이드 전에 생성한 스냅샷으로 롤백할 수 있습니다. [업그레이드 실패 시 VMware Cloud Director 장치 롤백](#)의 내용을 참조하십시오.

VMware Update Repository를 사용하여 VMware Cloud Director 장치 업그레이드

VMware Update Repository를 사용하여 VMware Cloud Director 장치를 버전 9.7에서 버전 10.0 이상으로 업그레이드하거나 패치를 적용할 수 있습니다.

참고 VMware Update Repository는 VMware Cloud Director를 최신 VMware Cloud Director 버전으로 업그레이드하는 데만 사용할 수 있습니다. VMware Update Repository에서는 최신 버전만 사용할 수 있습니다. VMware Cloud Director를 다른 버전으로 업그레이드하려면 [업데이트 패키지를 사용하여 VMware Cloud Director 장치 업그레이드](#) 항목을 참조하십시오.

VMware Cloud Director 장치 배포를 업그레이드하는 동안 VMware Cloud Director 서비스가 작동을 중지하고 다운타임이 발생할 수 있습니다. 다운타임은 각 VMware Cloud Director 장치를 업그레이드하고 VMware Cloud Director 데이터베이스 업그레이드 스크립트를 실행하는 데 필요한 시간에 따라 달라집니다. VMware Cloud Director 서버 그룹의 작업 셀 수는 마지막 VMware Cloud Director 장치에서 VMware Cloud Director 서비스를 중지할 때까지 줄어듭니다. VMware Cloud Director HTTP 끝점 앞에 올바르게 구성된 로드 밸런서는 중지된 셀에 대한 트래픽 라우팅을 중지해야 합니다.

모든 VMware Cloud Director 장치에 업그레이드를 적용하고 데이터베이스 업그레이드가 완료된 후에는 각각의 VMware Cloud Director 장치를 재부팅해야 합니다.

사전 요구 사항

- 기본 VMware Cloud Director 장치의 스냅샷을 생성합니다.
 - a 버전 10.1 이상에서 업그레이드하거나 패치를 적용할 때 기본 데이터베이스 서비스 장애가 발생하는 경우 자동 페일오버를 사용하도록 설정하는 경우, 업그레이드 기간 동안 페일오버 모드를 Manual로 변경합니다. 업그레이드 후에는 페일오버 모드를 Automatic으로 설정할 수 있습니다. [VMware Cloud Director 장치의 자동 페일오버](#)의 내용을 참조하십시오.
 - b 데이터베이스 고가용성 클러스터의 기본 VMware Cloud Director 장치가 있는 vCenter Server 인스턴스에 로그인합니다.
 - c 기본 VMware Cloud Director 장치로 이동하여 해당 장치를 마우스 오른쪽 버튼으로 클릭한 다음 **전원 > 게스트 OS 종료**를 클릭합니다.
 - d 장치를 마우스 오른쪽 버튼으로 클릭하고 **스냅샷 > 스냅샷 생성**을 클릭합니다. 스냅샷의 이름과 설명(선택 사항)을 입력하고 **확인**을 클릭합니다.
 - e VMware Cloud Director 장치를 마우스 오른쪽 버튼으로 클릭하고 **전원 > 전원 켜기**를 클릭합니다.
 - f 데이터베이스 고가용성 구성의 모든 노드가 정상 상태인지 확인합니다. [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.
- VMware Cloud Director 장치가 <https://vapp-updates.vmware.com>에 액세스할 수 있는지 확인합니다.

절차

- 1 웹 브라우저에서 VMware Cloud Director 장치 인스턴스의 장치 관리 사용자 인터페이스에 로그인하여 기본 장치를 식별합니다(https://appliance_ip_address:5480).

기본 장치 이름을 기록해 둡니다. 데이터베이스를 백업할 때는 기본 장치를 사용해야 합니다.

- 2 기본 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 3 VMware Update Repository를 가리키도록 업데이트 저장소를 재설정합니다.

```
vamicli update --repo ""
```

- 4 업데이트를 확인하여 VMware Update Repository에 원하는 업그레이드가 있는지 확인합니다.
기본적으로 vamicli 명령은 VMware Update Repository를 가리킵니다.

```
vamicli update --check
```

업그레이드 릴리스가 사용 가능한 업데이트로 표시됩니다.

- 5 다음 명령을 실행하여 VMware Cloud Director를 종료합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 6 기본 장치에서 계속 진행하여 VMware Cloud Director 장치에 내장된 데이터베이스를 백업합니다.

```
/opt/vmware/appliance/bin/create-db-backup
```

참고 장치는 한 번만 백업해야 합니다. 사용 가능한 업그레이드를 적용한 후에는 장치를 백업하지 마십시오.

- 7 사용 가능한 업그레이드를 적용합니다.

```
vamicli update --install latest
```

- 8 나머지 대기 및 애플리케이션 셀에 로그인하고 각 장치에서 3, 4, 5 및 7단계를 반복합니다.
- 9 임의 장치에서 VMware Cloud Director 데이터베이스 upgrade 유틸리티를 실행합니다.

```
/opt/vmware/vcloud-director/bin/upgrade
```

- 10 각 VMware Cloud Director 장치를 재부팅합니다.

```
shutdown -r now
```

다음에 수행할 작업

- 업그레이드에 성공하면 VMware Cloud Director 장치의 스냅샷을 삭제할 수 있습니다.
- 업그레이드에 성공하지 못하면 VMware Cloud Director 장치를 업그레이드 전에 생성한 스냅샷으로 롤백할 수 있습니다. [업그레이드 실패 시 VMware Cloud Director 장치 롤백](#)의 내용을 참조하십시오.

- `vamicli update --install latest` 명령이 실패하는 경우 VMware Cloud Director의 최신 업데이트 설치 실패의 내용을 참조하십시오.

업그레이드 실패 시 VMware Cloud Director 장치 롤백

VMware Cloud Director 장치 업그레이드가 실패하는 경우 업그레이드 전에 생성한 장치의 스냅샷을 사용하여 VMware Cloud Director 장치를 롤백할 수 있습니다.

롤백을 시작하기 전에 VMware Cloud Director 장치 API를 사용하여 클러스터의 대기 노드의 노드 ID를 기록해 둡니다. <http://code.vmware.com>에서 "VMware Cloud Director 장치 API 스키마 참조"의 내용을 참조하십시오.

- 1 기본 VMware Cloud Director 장치를 업그레이드 시작 전에 생성한 스냅샷으로 되돌립니다.
되돌리기 옵션을 사용하여 가상 시스템 스냅샷을 복원하는 방법을 읽으십시오. "vSphere 가상 시스템 관리 가이드"에서 [복구를 사용하여 VM 스냅샷 복원](#)을 참조하십시오.
- 2 기본 VMware Cloud Director 장치 셀의 전원을 끕니다.
- 3 각 VMware Cloud Director 장치 셀의 OS에 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다. **root** 사용자로 로그인해야 합니다.
- 4 모든 장치 셀에서 VMware Cloud Director 서비스를 중지합니다.

```
service vmware-vcd stop
```

- 5 기본 VMware Cloud Director 셀을 사용하여 클러스터의 보조 노드를 등록 취소합니다.
 - a 기본 셀의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
 - b 사용자를 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

- c 명령을 실행하여 대기 장치 셀을 등록 취소합니다.
실행 중이 아닌 대기 노드의 등록을 취소하려면 노드 ID를 제공해야 합니다.

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister --node-id=노드 ID -f /opt/vmware/vpostgres/current/etc/repmgr.conf
```

- d 5.c를 반복하여 다른 대기 장치 셀의 등록을 취소합니다.
- 6 vSphere Client에서 모든 대기 장치를 종료하고 삭제합니다.
 - a vSphere Client에서 대기 장치로 이동합니다.
 - b 대기 장치를 마우스 오른쪽 버튼으로 클릭하고 **전원 > 게스트 OS 종료**를 클릭합니다.
 - c 장치를 마우스 오른쪽 버튼으로 클릭하고 **디스크에서 삭제**를 클릭합니다.
 - d 다른 대기 장치 셀에 대해 6.c에서 6.a까지 반복합니다.

- 7 repmgr 도구 제품군과 기본 VMware Cloud Director 장치 셀의 내장형 PostgreSQL 데이터베이스가 제대로 작동하는지 확인합니다.

a 사용자를 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

b 명령을 실행하여 클러스터 상태를 확인합니다.

```
/opt/vmware/vpostgres/current/bin/repmgr cluster show
```

콘솔 출력에 클러스터의 유일한 노드에 대한 정보가 표시됩니다.

```

      ID | Name      | Role   | Status           | Upstream | Location | Connection
string
-----+-----+-----+-----+-----+-----+-----
+-----+-----+-----+-----+-----+-----+-----
Node 1 | 노드 이름 | primary | *running        |          | default | host=호스트 IP 주소
user=repmgr dbname=repmgr

```

- 8 보조 장치를 다시 배포합니다. **vSphere Client**를 사용하여 **VMware Cloud Director** 장치 배포의 내용을 참조하십시오.
- 9 각 VMware Cloud Director 장치 셀의 OS에 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다. **root** 사용자로 로그인해야 합니다.
- 10 VMware Cloud Director 서비스를 시작합니다.

```
service vmware-vcd start
```

외부 PostgreSQL 데이터베이스를 사용하는 VMware Cloud Director를 VMware Cloud Director 장치에 마이그레이션

현재 VMware Cloud Director 환경에서 외부 PostgreSQL 데이터베이스를 사용하는 경우에는 VMware Cloud Director 장치 배포로 구성된 새 VMware Cloud Director 환경으로 마이그레이션할 수 있습니다. 현재 VMware Cloud Director 환경은 Linux에 설치된 VMware Cloud Director 또는 VMware Cloud Director 장치 배포로 구성될 수 있습니다. 새로운 VMware Cloud Director 환경은 고가용성 모드의 장치 내장형 PostgreSQL 데이터베이스를 사용할 수 있습니다.

마이그레이션 워크플로에는 4가지 주요 단계가 포함되어 있습니다.

- 기존 VMware Cloud Director 환경 업그레이드
- 하나 이상의 VMware Cloud Director 장치 인스턴스를 배포하여 새 VMware Cloud Director 서버 그룹 생성
- 외부 데이터베이스를 내장형 데이터베이스로 마이그레이션
- 공유 전송 서비스 데이터 및 인증서 데이터 복사

절차

- 1 현재 외부 PostgreSQL 데이터베이스의 버전이 9.x인 경우 외부 PostgreSQL 데이터베이스를 버전 10 이상으로 업그레이드합니다.

- 2 현재 VMware Cloud Director 환경을 버전 10.2로 업그레이드합니다.

[Linux에서 VMware Cloud Director 업그레이드](#)의 내용을 참조하십시오.

- 3 마이그레이션 소스 VMware Cloud Director 다시 시작이 성공했는지 확인합니다.
- 4 업그레이드된 VMware Cloud Director 환경의 각 셀에서 다음 명령을 실행하여 VMware Cloud Director 서비스를 중지합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <관리자 이름> cell --shutdown
```

- 5 외부 PostgreSQL 데이터베이스에서 현재 데이터베이스를 백업합니다.

```
sudo -u postgres path_to_pg_dump -Fc db_name > /tmp/db_dump_name
```

/tmp 폴더에 사용 가능한 공간이 충분하지 않은 경우 다른 위치를 사용하여 덤프 파일을 저장합니다.

- 6 데이터베이스 소유자 및 데이터베이스 이름이 vcloud와 다르면 사용자 이름 및 데이터베이스 이름을 기록해 둡니다.

[13단계](#)에서 새 환경에 이 사용자를 생성하고 데이터베이스의 이름을 변경해야 합니다.

- 7 새 VMware Cloud Director 환경에서 기존 환경의 IP 주소를 사용하도록 하려면 속성 및 인증서 파일을 외부 PostgreSQL 데이터베이스의 위치에 복사하고 셀의 전원을 꺼야 합니다.

- a /opt/vmware/vcloud-director/etc/에 있는 global.properties, responses.properties, certificates, proxycertificates, truststore 파일을 외부 PostgreSQL 데이터베이스의 /tmp 또는 원하는 위치에 복사합니다.

- b 기존 환경에서 셀의 전원을 끕니다.

- 8 새 VMware Cloud Director 환경이 기존 환경의 NFS 서버를 사용하도록 하려면 새 공유 NFS 마운트 지점으로 이 NFS 서버의 새 디렉토리를 생성하고 내보냅니다.

이전 NFS에 있는 사용자의 사용자 및 그룹 ID(UID/GID)가 새 NFS에 있는 사용자 및 그룹 ID와 일치하지 않을 수 있기 때문에 기존 마운트 지점을 재사용 할 수 없습니다.

- 9 하나 이상의 VMware Cloud Director 장치 인스턴스를 배포하여 새 서버 그룹을 생성합니다.

- 데이터베이스고가용성 기능을 사용하려는 경우, 기본 셀 하나와 두 개의 대기 셀, 그리고 선택적으로 하나 이상의 vCD 애플리케이션 셀을 배포합니다.
- 기존 환경의 셀 전원을 끄면 원래 IP 주소를 새 셀에 사용할 수 있습니다.
- 기존 NFS 서버에서 새 경로를 내보낸 경우 새 환경에 대해 이 새 공유 마운트 지점을 사용할 수 있습니다.

[VMware Cloud Director 장치의 배포 및 초기 구성](#)의 내용을 참조하십시오.

- 10 새로 배포된 각 셀에서 다음 명령을 실행하여 VMware Cloud Director 서비스를 중지합니다.

```
service vmware-vcd stop
```

- 11 외부 PostgreSQL 데이터베이스의 /tmp폴더에서 새 환경의 기본 셀에 있는 /tmp 폴더로 덤프 파일을 복사합니다.

5단계를 참조하십시오.

- 12 덤프 파일에 대한 사용 권한을 변경합니다.

```
chmod a+r /tmp/db_dump_name
```

- 13 새로 배포된 기본 셀의 콘솔에 **root**로 로그인하고 외부에서 내장된 데이터베이스로 VMware Cloud Director 데이터베이스를 전송합니다.

- a 사용자를 postgres로 전환하고 psql 데이터베이스 터미널에 연결한 다음, 명령문을 실행하여 vcloud 데이터베이스를 삭제합니다.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

- b 기존 외부 데이터베이스의 데이터베이스 소유자가 vcloud와 다른 경우에는 6단계에서 적어둔 이름으로 사용자를 생성합니다.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'CREATE USER  
<db_owner_external_pg>;'
```

- c pg_restore 명령을 실행합니다.

```
sudo -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/  
db_dump_name
```

- d 기존 외부 데이터베이스의 데이터베이스 이름이 vcloud와 다른 경우에는 6단계에서 적어둔 이름을 사용하여 데이터베이스 이름을 vcloud로 변경합니다.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE  
<db_name_external_pg> RENAME TO vcloud;'
```

- e 기존 VMware Cloud Director 환경의 데이터베이스 소유자가 vcloud와 다르다면 데이터베이스 소유자를 vcloud로 변경하고 테이블을 vcloud에 다시 할당합니다.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE vcloud  
OWNER TO vcloud;'
```

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -d vcloud -c 'REASSIGN  
OWNED BY <db_owner_external_pg> TO vcloud;'
```

- 14 새로 배포된 각 셀에서 구성 데이터를 백업하고 바꾼 후 VMware Cloud Director 서비스를 재구성하고 시작합니다.

- a 속성, **truststore** 및 인증서 파일을 백업하고, **7 a단계**에서 파일을 복사한 마이그레이션 소스의 외부 PostgreSQL 데이터베이스 위치에서 이 파일을 복사하여 교체합니다.

global.properties, responses.properties, truststore, certificates 및 proxycertificates 파일은 /opt/vmware/vcloud-director/etc/에 있습니다.

- b /opt/vmware/vcloud-director/certificates.ks에 있는 키 저장소 파일을 백업합니다.
마이그레이션 소스에서 키 저장소 파일을 복사하여 교체하지 마십시오.

- c 다음 명령을 실행하여 VMware Cloud Director 서비스를 재구성합니다.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type
postgres --database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --
database-port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-
director/certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

여기서:

- --keystore-password 값은 이 장치의 초기 **root** 암호와 일치합니다.
- --database-password 값은 장치 배포 중에 설정한 데이터베이스 암호와 일치합니다.
- --database-host 값은 기본 장치의 eth1 네트워크 IP 주소와 일치합니다.
- --primary-ip 값은 장치의 eth0 네트워크 IP 주소와 일치합니다.
- --console-proxy-ip 값은 장치의 eth0 네트워크 IP 주소와 일치합니다.
- --console-proxy-port 값은 장치 콘솔 프록시 포트 **8443**과 일치합니다.

문제 해결에 대한 자세한 내용은 **VMware Cloud Director 장치에 마이그레이션하거나 복원할 때 VMware Cloud Director 서비스를 재구성하지 못함** 항목을 참조하십시오.

- d 다음 명령을 실행하여 VMware Cloud Director 서비스를 시작합니다.

```
service vmware-vcd start
```

셀 시작의 진행률은 /opt/vmware/vcloud-director/logs/cell.log에서 모니터링할 수 있습니다.

- 15 HTTP, HTTPS 및 TCP 트래픽에 대한 로드 밸런서 풀에 모든 새 장치 eth0 IP를 포함하도록 로드 밸런서 구성을 수정하고 해당 풀에서 이전 Linux VMware Cloud Director 셀 IP를 제거합니다.

- 16 새 서버 그룹의 모든 셀이 시작 프로세스를 완료하면 VMware Cloud Director 환경의 마이그레이션이 성공했는지 확인합니다.
 - a 새 서버 그룹의 임의 셀의 eth0 네트워크 IP 주소(https://eth0_IP_new_cell/provider)를 사용하여 Service Provider Admin Portal을 엽니다.
 - b 마이그레이션 소스의 기존 **시스템 관리자** 자격 증명을 사용하여 Service Provider Admin Portal에 로그인합니다.
 - c 새 환경에서 vSphere 및 클라우드 리소스를 사용할 수 있는지 확인합니다.
- 17 VMware Cloud Director 마이그레이션을 확인한 후에는 Service Provider Admin Portal을 사용하여 이전 VMware Cloud Director 환경에 속하는 연결이 끊어진 셀을 삭제합니다.
 - a 위쪽 탐색 모음의 **리소스**에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **클라우드 셀**을 클릭합니다.
 - c 비활성 셀을 선택하고 **등록 취소**를 클릭합니다.

VMware Cloud Director 장치를 배포하고 마이그레이션된 환경의 서버 그룹에 멤버를 추가할 수 있습니다.

후속 작업

새로 마이그레이션한 VMware Cloud Director 장치 환경에서 자체 서명된 인증서를 사용합니다. 이전 환경에서 잘 서명된 인증서를 사용하려면 새 환경의 각 셀에서 다음 단계를 수행합니다.

- 1 키 저장소 파일을 이전 셀에서 `/opt/vmware/vcloud-director/data/transfer/certificates.ks`로 복사하여 교체합니다.
- 2 셀 관리 도구 명령을 실행하여 인증서를 교체합니다.

vcloud.vcloud가 이 파일의 소유자인지 확인합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/data/transfer/certificates.ks \
--keystore-password ks_password_old_vCD
```

- 3 VMware Cloud Director 서비스를 다시 시작합니다.

```
service vmware-vcd restart
```

이 서버 그룹에 새 구성원을 추가하는 경우 이렇게 잘 서명된 인증서를 사용하여 새 장치 셀이 배포됩니다.

VMware Cloud Director 업그레이드 후 작업

모든 VMware Cloud Director 서버 및 공유 데이터베이스를 업그레이드한 후에는 클라우드에 네트워크 서비스를 제공하는 NSX Manager 인스턴스를 업그레이드할 수 있습니다. 그런 다음, VMware Cloud Director 설치에 등록되어 있는 vCenter Server 인스턴스 및 ESXi 호스트를 업그레이드할 수 있습니다.

중요 VMware Cloud Director는 고급 Edge 게이트웨이만 지원합니다. 고급이 아닌 레거시 Edge 게이트웨이는 고급 게이트웨이로 변환해야 합니다. <https://kb.vmware.com/kb/66767>의 내용을 참조하십시오.

버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)의 내용을 참조하십시오.

중요 버전 10.1 이상으로 업그레이드한 후 VMware Cloud Director는 연결된 모든 인프라 끝점에 대한 인증서를 항상 확인합니다. 이는 VMware Cloud Director가 SSL 인증서를 관리하는 방식이 변경되었기 때문입니다. 업그레이드 전에 인증서를 VMware Cloud Director로 가져오지 않으면 SSL 확인 문제로 인해 vCenter Server 및 NSX 연결에 실패한 연결 오류가 표시될 수 있습니다. 이 경우 업그레이드 후 다음 두 가지 옵션이 제공됩니다.

- 1 셸 관리 도구 `trust-infra-certs` 명령을 실행하여 모든 인증서를 중앙 집중식 인증서 저장소로 자동으로 가져옵니다. [vSphere 리소스에서 끝점 인증서 가져오기](#)를 참조하십시오.
- 2 Service Provider Admin Portal UI에서 각 vCenter Server 및 NSX 인스턴스를 선택하고 인증서를 수락하는 동안 자격 증명을 다시 입력합니다.

연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager 업그레이드

VMware Cloud Director에 등록된 ESXi 호스트와 vCenter Server를 업그레이드하기 전에 해당 vCenter Server에 연결된 각 NSX Manager를 업그레이드해야 합니다.

NSX Manager를 업그레이드하면 NSX 관리 기능에 대한 액세스가 중단되지만 네트워크 서비스는 중단되지 않습니다. VMware Cloud Director 셸이 실행 중인지 여부에 관계없이 VMware Cloud Director 업그레이드를 전후하여 NSX Manager를 업그레이드할 수 있습니다.

NSX 업그레이드에 대한 자세한 내용은 <https://docs.vmware.com>의 NSX for vSphere 설명서를 참조하십시오.

절차

- 1 VMware Cloud Director 설치에 등록된 각 vCenter Server에 연결되어 있는 NSX Manager를 업그레이드합니다.

- 2 모든 NSX Manager를 업그레이드한 후에는 등록된 vCenter Server 시스템과 ESXi 호스트를 업그레이드할 수 있습니다.

vCenter Server 시스템, ESXi 호스트 및 NSX Edge 업그레이드

VMware Cloud Director 및 NSX Manager를 업그레이드한 후에는 VMware Cloud Director에 등록되어 있는 vCenter Server 시스템 및 ESXi 호스트를 업그레이드해야 합니다. 연결된 모든 vCenter Server 시스템과 ESXi 호스트를 업그레이드한 후에 NSX Edge를 업그레이드할 수 있습니다.

사전 요구 사항

클라우드에 연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager를 이미 업그레이드했는지 확인합니다. 연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager 업그레이드의 내용을 참조하십시오.

절차

- 1 vCenter Server 인스턴스를 비활성화합니다.
 - a VMware Cloud Director Service Provider Admin Portal의 위쪽 탐색 모음의 **리소스**에서 **vSphere 리소스**를 선택합니다.
 - b 왼쪽 패널에서 **vCenter Server 인스턴스**를 클릭합니다.
 - c 비활성화할 vCenter Server 인스턴스 옆에 있는 라디오 버튼을 선택하고 **사용 안 함**을 클릭합니다.
 - d **확인**을 클릭합니다.
- 2 vCenter Server 시스템을 업그레이드합니다.

자세한 내용은 "vCenter Server 업그레이드" 를 참조하십시오.
- 3 모든 VMware Cloud Director 공용 URL 및 인증서 체인을 확인합니다.
 - a 위쪽 탐색 모음에서 **관리**를 선택합니다.
 - b 왼쪽 패널의 **설정** 아래에서 **공개 주소**를 클릭합니다.
 - c 모든 공개 주소를 확인합니다.
- 4 VMware Cloud Director에서 vCenter Server 등록을 새로 고칩니다.
 - a VMware Cloud Director Service Provider Admin Portal의 위쪽 탐색 모음의 **리소스**에서 **vSphere 리소스**를 선택합니다.
 - b 왼쪽 패널에서 **vCenter Server 인스턴스**를 클릭합니다.
 - c 대상 vCenter Server 옆에 있는 라디오 버튼을 선택하고 **다시 연결**을 클릭합니다.
 - d **확인**을 클릭합니다.

5 업그레이드된 vCenter Server 시스템이 지원하는 각 ESXi 호스트를 업그레이드합니다.

"VMware ESXi 업그레이드" 를 참조하십시오.

중요 클라우드에 속한 가상 시스템을 지원할 정도로 업그레이드된 호스트의 용량이 충분한지 확인하려면 호스트를 몇 개씩 업그레이드하십시오. 이렇게 하면 Host Agent 업그레이드를 지정된 시간에 완료하여 가상 시스템을 업그레이드된 호스트로 다시 마이그레이션할 수 있습니다.

- a vCenter Server 시스템을 사용하여 호스트를 유지 보수 모드로 설정하고, 해당 호스트의 모든 가상 시스템을 다른 호스트에 마이그레이션할 수 있도록 허용합니다.
 - b 호스트를 업그레이드합니다.
 - c vCenter Server 시스템을 사용하여 호스트를 다시 연결합니다.
 - d vCenter Server 시스템을 사용하여 호스트의 유지 보수 모드를 해제합니다.
- 6 (선택 사항) 업그레이드된 vCenter Server 시스템과 연결된 NSX Manager에서 관리하는 NSX Edge를 업그레이드합니다.

NSX Edge를 업그레이드하면 성능과 통합이 향상됩니다. NSX Manager 또는 VMware Cloud Director를 사용하여 NSX Edge를 업그레이드할 수 있습니다.

- NSX Manager를 사용하여 NSX Edge 업그레이드에 대한 자세한 내용은 <https://docs.vmware.com/kr/>의 NSX for vSphere 설명서를 참조하십시오.
- VMware Cloud Director를 사용하여 NSX Edge 게이트웨이를 업그레이드하려면 Edge에서 지원하는 VMware Cloud Director 네트워크 개체에서 작업해야 합니다.
 - VMware Cloud Director 또는 VMware Cloud Director API를 사용하여 Edge 게이트웨이가 서비스하는 네트워크를 재설정할 경우 Edge 게이트웨이가 자동으로 적절하게 업그레이드됩니다.
 - Edge 게이트웨이를 재배포하면 연결된 NSX Edge 어플라이언스가 업그레이드됩니다.

참고 다시 배포는 NSX Data Center for vSphere Edge 게이트웨이에만 지원됩니다.

- vApp의 컨텍스트 내에서 vApp 네트워크를 재설정하면 해당 네트워크와 연결된 NSX Edge 어플라이언스가 업그레이드됩니다. vApp 컨텍스트 내에서 vApp 네트워크를 재설정하려면 vApp의 **네트워크** 탭으로 이동하여 해당 네트워킹 세부 정보를 표시하고 vApp 네트워크 이름 옆에 있는 라디오 버튼을 클릭한 후 **재설정**을 클릭합니다.

Edge 게이트웨이 다시 배포 및 vApp 네트워크 재설정 방법에 대한 자세한 내용은 "VMware Cloud Director API 프로그래밍 가이드"의 내용을 참조하십시오.

다음에 수행할 작업

VMware Cloud Director 설치 환경에 등록된 다른 vCenter Server 시스템에 대해 이 절차를 반복합니다.

VMware Cloud Director 장치 관리

데이터베이스 HA 클러스터에 있는 셀의 상태를 볼 수 있고, 내장된 데이터베이스를 백업 및 복원할 수 있으며, 장치 설정을 재구성할 수 있습니다.

VMware Cloud Director 장치를 배포한 후에는 장치의 eth0 및 eth1 네트워크 IP 주소나 호스트 이름을 변경할 수 없습니다. VMware Cloud Director 장치에 다른 주소나 호스트 이름을 사용하려면 새 장치를 배포해야 합니다.

데이터베이스 고가용성 클러스터를 종료해야 하는 장치에 대해 유지 보수를 수행해야 하는 경우, 동기화 문제를 방지하려면 먼저 기본 장치를 종료한 다음 대기 장치를 종료해야 합니다.

참고 클러스터가 자동 페일오버에 대해 구성되어 있다면 하나 이상의 추가 셀을 배포한 후 장치 API를 사용하여 클러스터 페일오버 모드를 Automatic으로 재설정해야 합니다. [VMware Cloud Director 장치 API](#)를 참조하십시오. 새 셀에 대한 기본 페일오버 모드는 Manual입니다. 클러스터의 노드 전체에서 페일오버 모드가 일관되지 않은 경우 클러스터 페일오버 모드는 Indeterminate입니다. Indeterminate 모드는 이전 기본 셀 이후 노드와 기타 노드 간에 일관성 없는 클러스터 상태를 초래할 수 있습니다. 클러스터 페일오버 모드를 보려면 [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.

VMware Cloud Director 장치의 내장된 데이터베이스 백업 및 복원

VMware Cloud Director 장치 내장형 PostgreSQL 데이터베이스를 백업할 수 있으며, 이렇게 하면 장애 후 VMware Cloud Director 환경을 복원하는 데 도움이 됩니다.

VMware Cloud Director 장치 내장형 데이터베이스 백업

PostgreSQL 데이터베이스가 내장된 VMware Cloud Director 장치 배포로 환경이 구성된 경우 기본 셀에서 VMware Cloud Director 데이터베이스를 백업할 수 있습니다. 생성된 .tgz 파일은 NFS 공유 전송 서비스 스토리지 위치에 저장됩니다.

절차

- 1 기본 셀에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 다음 명령을 실행하여 VMware Cloud Director 장치 내장형 데이터베이스를 백업합니다.

```
/opt/vmware/appliance/bin/create-db-backup
```

결과

NFS 공유 전송 서비스 스토리지의 `vcloudapp.nfs_mount.VMware_vCloud_Director/pgdb-backup/` 디렉토리에서 새로 생성된 `db-backup-date_time_format.tgz` 파일을 볼 수 있습니다. .tgz 파일에는 기본 셀의 데이터베이스 덤프 파일, `global.properties`, `responses.properties`, `certificates`, `proxycertificates` 및 `truststore` 파일이 포함됩니다.

고가용성 데이터베이스 구성을 통해 VMware Cloud Director 장치 10.2.1 이하 환경 복원

HA 데이터베이스 구성을 사용하여 VMware Cloud Director 장치 10.2.1 이하 환경의 내장형 PostgreSQL 데이터베이스를 백업한 경우, 새 장치 클러스터를 배포하고 그 안에 장치 데이터베이스를 복원할 수 있습니다.

복원 워크플로에는 세 가지 주요 단계가 포함됩니다.

- 전송 서비스 NFS 공유 스토리지에서 내장된 데이터베이스 백업 .tar 파일 복사.
- 데이터베이스를 내장된 데이터베이스 기본 및 대기 셀로 복원.
- 필요한 애플리케이션 셀 배포.

사전 요구 사항

- 내장형 PostgreSQL 데이터베이스의 백업 .tar 파일이 있는지 확인합니다. [VMware Cloud Director 장치 내장형 데이터베이스 백업](#)의 내용을 참조하십시오.
- 기본 데이터베이스 셀 하나와 대기 데이터베이스 셀 두 개를 배포합니다. [VMware Cloud Director 장치의 배포 및 초기 구성](#)의 내용을 참조하십시오.
- 새 장치 클러스터가 이전 환경의 NFS 서버를 사용하도록 하려면, NFS 서버에서 새 공유로 새 디렉토리를 생성하고 내보냅니다. 기존 마운트 지점은 재사용할 수 없습니다.

절차

- 1 기본 및 대기 셀에서 **root**로 로그인하고 다음 명령을 실행하여 VMware Cloud Director 서비스를 중지합니다.

```
service vmware-vcd stop
```

- 2 기본 및 대기 셀에서 백업 .tar 파일을 /tmp 폴더에 복사합니다.
/tmp 폴더에 사용 가능한 공간이 충분하지 않은 경우 다른 위치를 사용하여 .tar 파일을 저장합니다.
- 3 기본 및 대기 셀에서 /tmp에 tar 백업 파일의 압축을 풉니다.

```
tar -zxvf db-backup-date_time_format.tgz
```

/tmp 폴더에서 추출된 global.properties, responses.properties, certificates, proxycertificates, truststore 및 vcloud_date_time_format이라는 데이터베이스 덤프 파일을 볼 수 있습니다.

참고 truststore 파일은 VMware Cloud Director 버전 9.7.0.1 ~ 버전 10.2.1에서만 사용할 수 있습니다.

4 기본 셀에서만 **root**로 콘솔에 로그인하여 다음 명령을 실행합니다.

- a vcloud 데이터베이스를 삭제합니다.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

- b pg_restore 명령을 실행합니다.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/vcloud_date_time_name
```

5 기본 및 대기 셀에서 구성 데이터 파일의 복사본을 저장하고 교체하고 재구성하여 VMware Cloud Director 서비스를 시작합니다.

- a 속성, 인증서 및 truststore 파일을 백업합니다.

global.properties, responses.properties, certificates, proxycertificates 및 truststore 파일은 /opt/vmware/vcloud-director/etc/에 있습니다.

참고 truststore 파일은 VMware Cloud Director 버전 9.7.0.1 ~ 버전 10.2.1에서만 사용할 수 있습니다.

```
cd /opt/vmware/vcloud-director/etc
mkdir -p backup
cp global.properties responses.properties certificates proxycertificates truststore backup
```

- b 3단계에서 추출한 백업 파일의 속성, 인증서 및 truststore 파일을 복사하여 교체합니다.

```
cd /tmp
cp global.properties responses.properties certificates proxycertificates truststore /opt/vmware/vcloud-director/etc/.
```

참고 truststore 파일은 VMware Cloud Director 버전 9.7.0.1 ~ 버전 10.2.1에서만 사용할 수 있습니다.

- c /opt/vmware/vcloud-director/certificates.ks에 있는 키 저장소 파일을 백업합니다.

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

- d 다음 명령을 실행하여 VMware Cloud Director 서비스를 재구성합니다.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type postgres --database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --
```

```
database-port 5432 \
--database-name vcloud --uuid --keystore /opt/vmware/vcloud-director/certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-ssl true
```

여기서:

- --keystore-password 옵션은 장치의 인증서에 대한 키 저장소 암호와 일치합니다. 키 저장소 암호는 장치 배포 중에 사용한 **root** 암호일 수 있습니다.
- --database-password 옵션은 VMware Cloud Director 장치 관리 UI(https://appliance_eth0_ip:5480)에서 장치 설정 중에 설정한 데이터베이스 암호와 일치합니다.
- --database-host 옵션은 기본 데이터베이스 장치의 eth1 네트워크 IP 주소와 일치합니다.
- --primary-ip 값은 복원하는 장치 셀의 eth0 네트워크 IP 주소와 일치합니다. 이 주소는 기본 데이터베이스 셀 IP 주소가 아닙니다.
- --console-proxy-ip 옵션은 복원하는 장치의 eth0 네트워크 IP 주소와 일치합니다.

문제 해결에 대한 자세한 내용은 [VMware Cloud Director 장치에 마이그레이션하거나 복원할 때 VMware Cloud Director 서비스를 재구성하지 못함](#) 항목을 참조하십시오.

- e 다음 명령을 실행하여 VMware Cloud Director 서비스를 시작합니다.

```
service vmware-vcd start
```

셀 시작의 진행률은 /opt/vmware/vcloud-director/logs/cell.log에서 모니터링할 수 있습니다.

- 6 (선택 사항) 추가 애플리케이션 셀을 배포합니다. [VMware Cloud Director 장치의 배포 및 초기 구성](#)의 내용을 참조하십시오.
- 7 새 장치가 교체할 원래 장치와 다른 IP를 사용하는 경우 새 장치 IP를 포함하도록 VMware Cloud Director 서버 그룹 앞에 있는 로드 밸런서의 구성을 업데이트해야 합니다.
- 8 서버 그룹의 모든 셀이 시작 프로세스를 완료하면 VMware Cloud Director 환경의 복원이 성공했는지 확인합니다.
 - a 새 서버 그룹의 임의 셀의 eth0 네트워크 IP 주소(https://et0_IP_new_cell/provider)를 사용하여 VMware Cloud Director Service Provider Admin Portal을 엽니다.

7단계에 따라 로드 밸런서 구성을 업데이트한 경우 서버 그룹의 공용 주소를 사용하여 Service Provider Admin Portal에 액세스해야 합니다.
 - b 기존 **시스템 관리자** 자격 증명을 사용하여 Service Provider Admin Portal에 로그인합니다.
 - c 새 환경에서 vSphere 및 클라우드 리소스를 사용할 수 있는지 확인합니다.

- 9 데이터베이스 복원을 확인한 후에는 Service Provider Admin Portal을 사용하여 이전 VMware Cloud Director 환경에 속하는 연결이 끊어진 셀을 삭제합니다.
 - a 위쪽 탐색 모음의 리소스에서 클라우드 리소스를 선택합니다.
 - b 왼쪽 창에서 클라우드 셀을 클릭합니다.
 - c 비활성 셀을 선택하고 등록 취소를 클릭합니다.
- 10 복원 전 페일오버 모드가 Automatic이었던 경우 VMware Cloud Director 장치 API를 사용하여 다시 Automatic으로 설정해야 합니다.

고가용성 데이터베이스 구성을 통해 VMware Cloud Director 장치 10.2.2 이상 환경 복원

HA 데이터베이스 구성을 사용하는 VMware Cloud Director 장치 10.2.2 이상 환경의 내장형 PostgreSQL 데이터베이스를 백업한 경우, 새 장치 클러스터를 배포하고 그 안에 장치 데이터베이스를 복원할 수 있습니다.

복원 워크플로에는 세 가지 주요 단계가 포함됩니다.

- 전송 서비스 NFS 공유 스토리지에서 내장된 데이터베이스 백업 .tar 파일 복사.
- 데이터베이스를 내장된 데이터베이스 기본 및 대기 셀로 복원.
- 필요한 애플리케이션 셀 배포.

사전 요구 사항

- 내장형 PostgreSQL 데이터베이스의 백업 .tar 파일이 있는지 확인합니다. [VMware Cloud Director 장치 내장형 데이터베이스 백업](#)의 내용을 참조하십시오.
- 기본 데이터베이스 셀 하나와 대기 데이터베이스 셀 두 개를 배포합니다. [VMware Cloud Director 장치의 배포 및 초기 구성](#)의 내용을 참조하십시오.
- 새 장치 클러스터가 이전 환경의 NFS 서버를 사용하도록 하려면, NFS 서버에서 새 공유로 새 디렉토리를 생성하고 내보냅니다. 기존 마운트 지점은 재사용할 수 없습니다.

절차

- 1 기본 및 대기 셀에서 root로 로그인하고 다음 명령을 실행하여 VMware Cloud Director 서비스를 중지합니다.

```
service vmware-vcd stop
```

- 2 기본 및 대기 셀에서 백업 .tar 파일을 /tmp 폴더에 복사합니다.
/tmp 폴더에 사용 가능한 공간이 충분하지 않은 경우 다른 위치를 사용하여 .tar 파일을 저장합니다.
- 3 기본 및 대기 셀에서 /tmp에 tar 백업 파일의 압축을 풉니다.

```
tar -zxvf db-backup-date_time_format.tgz
```


/tmp 폴더에서 추출된 global.properties, responses.properties, certificates.pem, certificates.key, proxycertificates.pem, proxycertificates.key, truststore.pem 및 vcloud_date_time_format이라는 데이터베이스 덤프 파일을 볼 수 있습니다.

참고 truststore.pem 파일은 VMware Cloud Director 10.2.2 이상에서만 사용할 수 있습니다.

- 4 기본 셸에서만 **root**로 콘솔에 로그인하여 다음 명령을 실행합니다.

- a vcloud 데이터베이스를 삭제합니다.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

- b pg_restore 명령을 실행합니다.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/vcloud_date_time_name
```

- 5 기본 및 대기 셸에서 구성 데이터 파일의 복사본을 저장하고 교체하고 재구성하여 VMware Cloud Director 서비스를 시작합니다.

- a 속성, 인증서 및 truststore 파일을 백업합니다.

global.properties, responses.properties, certificates.pem, certificates.key, proxycertificates.pem, proxycertificates.key 및 truststore.pem 파일은 /opt/vmware/vcloud-director/etc/에 있습니다.

참고 truststore.pem 파일은 VMware Cloud Director 10.2.2 이상에서만 사용할 수 있습니다.

```
cd /opt/vmware/vcloud-director/etc
mkdir -p backup
cp global.properties responses.properties certificates.* proxycertificates.*
truststore.* backup
```

- b 3단계에서 추출한 백업 파일의 속성, 인증서 및 truststore 파일을 복사하여 교체합니다.

```
cd /tmp
cp global.properties responses.properties certificates.* proxycertificates.*
truststore.* /opt/vmware/vcloud-director/etc/
```

참고 truststore.pem 파일은 VMware Cloud Director 10.2.2 이상에서만 사용할 수 있습니다.

- c /opt/vmware/vcloud-director/certificates.ks에 있는 키 저장소 파일을 백업합니다.

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

- d 다음 명령을 실행하여 VMware Cloud Director 서비스를 재구성합니다.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type
postgres --database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --
database-port 5432 \
--database-name vcloud --uuid --keystore /opt/vmware/vcloud-director/certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443

/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
ssl true
```

여기서:

- --keystore-password 옵션은 장치의 인증서에 대한 키 저장소 암호와 일치합니다. 키 저장소 암호는 장치 배포 중에 사용한 **root** 암호일 수 있습니다.
- --database-password 옵션은 VMware Cloud Director 장치 관리 UI(https://appliance_eth0_ip:5480)에서 장치 설정 중에 설정한 데이터베이스 암호와 일치합니다.
- --database-host 옵션은 기본 데이터베이스 장치의 eth1 네트워크 IP 주소와 일치합니다.
- --primary-ip 값은 복원하는 장치 셀의 eth0 네트워크 IP 주소와 일치합니다. 이 주소는 기본 데이터베이스 셀 IP 주소가 아닙니다.
- --console-proxy-ip 옵션은 복원하는 장치의 eth0 네트워크 IP 주소와 일치합니다.

문제 해결에 대한 자세한 내용은 [VMware Cloud Director 장치에 마이그레이션하거나 복원할 때 VMware Cloud Director 서비스를 재구성하지 못함](#) 항목을 참조하십시오.

- e 다음 명령을 실행하여 VMware Cloud Director 서비스를 시작합니다.

```
service vmware-vcd start
```

셀 시작의 진행률은 `/opt/vmware/vcloud-director/logs/cell.log`에서 모니터링할 수 있습니다.

- 6 (선택 사항) 추가 애플리케이션 셀을 배포합니다. [VMware Cloud Director 장치의 배포 및 초기 구성](#)의 내용을 참조하십시오.
- 7 새 장치가 교체할 원래 장치와 다른 IP를 사용하는 경우 새 장치 IP를 포함하도록 VMware Cloud Director 서버 그룹 앞에 있는 로드 밸런서의 구성을 업데이트해야 합니다.
- 8 서버 그룹의 모든 셀이 시작 프로세스를 완료하면 VMware Cloud Director 환경의 복원이 성공했는지 확인합니다.

- a 새 서버 그룹의 임의 셀의 eth0 네트워크 IP 주소(https://et0_IP_new_cell/provider)를 사용하여 VMware Cloud Director Service Provider Admin Portal을 엽니다.

7단계에 따라 로드 밸런서 구성을 업데이트한 경우 서버 그룹의 공용 주소를 사용하여 Service Provider Admin Portal에 액세스해야 합니다.

- b 기존 **시스템 관리자** 자격 증명을 사용하여 Service Provider Admin Portal에 로그인합니다.
 - c 새 환경에서 vSphere 및 클라우드 리소스를 사용할 수 있는지 확인합니다.
- 9 데이터베이스 복원을 확인한 후에는 Service Provider Admin Portal을 사용하여 이전 VMware Cloud Director 환경에 속하는 연결이 끊어진 셀을 삭제합니다.
 - a 위쪽 탐색 모음의 **리소스**에서 **클라우드 리소스**를 선택합니다.
 - b 왼쪽 창에서 **클라우드 셀**을 클릭합니다.
 - c 비활성 셀을 선택하고 **등록 취소**를 클릭합니다.
- 10 복원 전 페일오버 모드가 Automatic이었던 경우 VMware Cloud Director 장치 API를 사용하여 다시 Automatic으로 설정해야 합니다.
- 11 복원 전에 VMware Cloud Director 장치 FIPS 모드가 켜져 있는 경우 VMware Cloud Director 장치 API를 사용하여 다시 설정해야 합니다.

셀 FIPS 모드는 자동으로 복원됩니다.

VMware Cloud Director 장치의 페일오버 모드 변경

기본적으로 VMware Cloud Director 장치는 수동 페일오버 모드에 있으며 기본 데이터베이스 서비스가 실패하면 페일오버 작업을 시작해야 합니다. 장치 API를 사용하여 페일오버 모드를 자동으로 변경할 수 있습니다.

VMware Cloud Director 10.1부터 기본 데이터베이스 서비스가 실패할 경우 VMware Cloud Director를 사용하도록 설정하여 새 기본으로 자동 페일오버를 수행할 수 있습니다. [VMware Cloud Director 장치의 자동 페일오버](#)의 내용을 참조하십시오.

페일오버 모드는 VMware Cloud Director 장치 API를 사용하여 automatic 또는 manual로 설정됩니다. [VMware Cloud Director 장치 API 스키마 참조](#)의 "페일오버 모드" 섹션을 참조하십시오.

자동 페일오버로 구성된 클러스터의 경우, 하나 이상의 추가 셀을 배포한 후 장치 API를 사용하여 클러스터의 페일오버 모드를 automatic으로 재설정해야 합니다. 클러스터의 페일오버 모드를 재설정하지 않으면 노드 전체의 페일오버 모드가 일치하지 않게 됩니다.

VMware Cloud Director 데이터베이스에 대한 외부 액세스 구성

특정 외부 IP 주소에서 기본 장치에 내장된 VMware Cloud Director 데이터베이스에 액세스할 수 있도록 설정할 수 있습니다.

VMware Cloud Director로 마이그레이션하는 동안 또는 타사 데이터베이스 백업 솔루션을 사용할 계획이면, 내장형 VMware Cloud Director 데이터베이스에 대한 외부 액세스를 사용하도록 설정할 수 있습니다.

절차

- 1 기본 셀에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 데이터베이스 디렉토리(/opt/vmware/appliance/etc/pg_hba.d/)로 이동합니다.

3 다음과 유사하게 대상 외부 IP 주소에 대한 항목을 포함하는 텍스트 파일을 생성합니다.

```
#TYPE DATABASE USER ADDRESS METHOD
host vcloud vcloud CIDR_notation md5
```

예는 다음과 같습니다.

```
#TYPE DATABASE USER ADDRESS METHOD
host vcloud vcloud 172.168.100.5/32 md5
host vcloud vcloud 172.168.20.5/32 md5
```

이 항목은 동적으로 업데이트되는 `pg_hba.conf` 파일에 추가되어, HA 클러스터의 기본 데이터베이스에 대한 액세스를 제어합니다.

VMware Cloud Director 장치에 대한 SSH 액세스 활성화 또는 비활성화

장치를 배포하는 동안 장치에 대한 SSH 액세스를 비활성화된 상태로 두거나 활성화할 수 있습니다. 배포 후에 SSH 액세스 설정을 전환할 수 있습니다.

SSH 데몬은 데이터베이스 HA 기능 및 원격 **루트** 로그인에 사용하기 위해 장치에서 실행됩니다. **루트** 사용자에 대한 SSH 액세스를 비활성화할 수 있습니다. 데이터베이스 HA 기능에 대한 SSH 액세스는 변경되지 않고 유지됩니다.

사전 요구 사항

OVF 속성을 영구적으로 변경하려면 vSphere UI를 사용하여 OVF 속성 값을 변경해야 합니다. "vSphere 가상 시스템 관리" 가이드에서 vApp 속성 구성 항목을 참조하십시오.

절차

- 예를 들어 테스트 목적으로 OVF 속성을 일시적으로 변경하려는 경우 VMware Cloud Director에서 속성을 변경합니다.
 - VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
 - 스크립트를 실행하여 SSH **루트** 액세스를 활성화 또는 비활성화합니다.
 - SSH **루트** 액세스를 활성화하려면 `/opt/vmware/appliance/bin/enable_root_login.sh` 스크립트를 실행합니다.
 - SSH **루트** 액세스를 비활성화하려면 `/opt/vmware/appliance/bin/disable_root_login.sh` 스크립트를 실행합니다.
- OVF 속성을 영구적으로 변경하려는 경우에는 vSphere 사용자 인터페이스를 사용하여 `vcloudapp.enable_ssh.VMware_vCloud_Director` 속성의 값을 설정합니다.

참고 vSphere의 속성 값을 변경하려면 VM의 전원을 꺼야 합니다.

- SSH를 활성화하려면 `vcloudapp.enable_ssh.VMware_vCloud_Director`의 값을 **True**로 설정합니다.

- SSH를 비활성화하려면 `vcloudapp.enable_ssh.VMware_vCloud_Director`의 값을 **False**로 설정합니다.

VMware Cloud Director 장치에서 FIPS 모드 활성화 또는 비활성화

버전 10.2.2부터는 FIPS 140-2 검증 암호화 모듈을 사용하고 FIPS 준수 모드에서 실행되도록 VMware Cloud Director 장치를 구성할 수 있습니다.

FIPS(Federal Information Processing Standard) 140-2는 암호화 모듈에 대한 보안 요구 사항을 규정하는 미국 및 캐나다 정부 표준입니다. NIST CMVP(암호화 모듈 검증 프로그램)는 FIPS 140-2 표준을 준수하는 암호화 모듈을 검증합니다.

VMware Cloud Director FIPS 지원의 목표는 다양한 규제 환경에서 규정 준수 및 보안 활동을 용이하게 하는 것입니다. VMware 제품의 FIPS 140-2 지원에 대해 자세히 알려면 <https://www.vmware.com/security/certifications/fips.html>을 참조하십시오.

VMware Cloud Director FIPS 검증 암호화는 기본적으로 비활성화되어 있습니다. FIPS 모드를 활성화하면 FIPS 140-2 검증 암호화 모듈을 사용하고 FIPS 준수 모드에서 실행되도록 VMware Cloud Director를 구성할 수 있습니다.

참고 FIPS 모드를 활성화하면 호스트 이름의 역방향 조회도 활성화됩니다.

중요 FIPS 모드를 활성화하면 vRealize Orchestrator와의 통합이 작동하지 않습니다.

VMware Cloud Director 10.2.2에서 FIPS 모드를 활성화하면 SAML 어설션을 암호화할 수 없습니다. FIPS 모드가 아니면 어설션 암호화에 대한 제한이 없습니다.

VMware Cloud Director는 다음과 같은 FIPS 140-2 검증 암호화 모듈을 사용합니다.

- VMware의 BC-FJA(Bouncy Castle FIPS Java API), 버전1.0.2.1: [Certificate #3673](#)
- VMware의 OpenSSL FIPS 개체 모듈, 버전 2.0.20-vmw: [Certificate #3857](#)

VMware Cloud Director는 CMT(셀 관리 도구)와 함께 번들로 제공됩니다. 하지만 셀 관리 도구는 FIPS를 준수하지 않습니다.

VMware Cloud Director 장치를 사용하는 경우 FIPS 준수 모드에서 실행되도록 장치를 구성하려면 장치 FIPS 모드와 셀 FIPS 모드를 모두 관리해야 합니다.

- 장치 FIPS 모드는 기본 장치 OS, 내장된 데이터베이스 및 다양한 시스템 라이브러리의 모드입니다.
- 셀 FIPS 모드는 각 장치에서 실행되는 VMware Cloud Director 셀의 모드입니다.

Linux에서 VMware Cloud Director의 FIPS 모드를 활성화 및 비활성화하려면 [서버 그룹의 셀에서 FIPS 모드 사용](#)을 참조하십시오.

사전 요구 사항

- 메트릭 수집을 활성화한 경우 Cassandra 인증서가 X.509 v3 인증서 표준을 따르고 필요한 모든 확장을 포함하는지 확인합니다. VMware Cloud Director가 사용하는 것과 동일한 암호 그룹으로 Cassandra를 구성해야 합니다. 허용되는 SSL 암호에 대한 자세한 내용은 [허용되는 SSL 암호화 목록 관리](#)를 참조하십시오.
- vCenter Lookup Service에서 VMware Cloud Director의 등록을 취소합니다. "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"의 [vSphere 서비스 구성](#)을 참조하십시오.

절차

- 1 Service Provider Admin Portal의 위쪽 탐색 모음에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **설정** 아래에서 **SSL**을 선택합니다.
- 3 **사용**을 클릭합니다.
- 4 프로세스를 시작하는 것을 확인하려면 **사용**을 클릭합니다.

구성이 완료되면 VMware Cloud Director에 사용 진행 중 (셀 다시 시작 대기 중) 메시지가 표시되고 5단계를 계속할 수 있습니다. 5단계에서 API 명령을 실행하면 VMware Cloud Director 장치가 자동으로 셀을 다시 시작합니다.

- 5 장치 FIPS 모드를 켜거나 끄려면 VMware Cloud Director 장치 API를 사용하여 `fips/{node_name}` URL에 PUT 요청을 합니다. [VMware Cloud Director 장치 API](#)를 참조하십시오.

참고 PUT 요청을 처리하는 시스템의 `{node_name}`을 사용해야 합니다.

예: FIPS 모드 활성화

요청:

```
PUT https://vcloud.example.com:5480/api/1.0.0/fips/{node_name}
Content-Type: application/json
...
{
  "applianceFips": "ON"
}
```

- 6 각 장치(예: 기본, 대기 및 애플리케이션 유형)에 대해 5단계를 반복합니다.

다음에 수행할 작업

셀의 상태를 확인하기 위해 VMware Cloud Director 장치 관리 UI를 사용할 수 있습니다. [VMware Cloud Director 장치 FIPS 모드 보기](#)의 내용을 참조하십시오.

VMware Cloud Director 장치 FIPS 모드 보기

버전 10.2.2부터는 VMware Cloud Director 장치를 FIPS 준수 모드에서 실행할 수 있습니다. 장치 및 셀 FIPS 모드를 볼 수 있습니다.

VMware Cloud Director 장치를 사용하는 경우 FIPS 준수 모드에서 실행되도록 VMware Cloud Director 장치를 구성하려면 장치 FIPS 모드와 셀 FIPS 모드를 모두 관리해야 합니다.

- 장치 FIPS 모드는 기본 장치 OS, 내장된 데이터베이스 및 다양한 시스템 라이브러리의 모드입니다.
- 셀 FIPS 모드는 각 장치에서 실행되는 VMware Cloud Director 셀의 모드입니다.

표 3-1. FIPS 모드 상태

전장	설명
	장치 및 셀 FIPS 모드가 일치합니다. 두 모드 모두 켜져 있거나 꺼져 있습니다.
	셀 FIPS 모드가 다시 시작 대기 중 상태입니다. 장치 API를 사용하여 장치 FIPS 모드를 활성화하거나 비활성화할 수 있습니다. 장치 FIPS 모드를 변경하면 VMware Cloud Director 셀 서비스가 자동으로 다시 시작됩니다.
	VMware Cloud Director 장치가 셀 FIPS 모드를 확인할 수 없습니다. 장치에서 VMware Cloud Director 서비스에 장애가 발생하면 셀 FIPS 모드가 확인되지 않을 수 있습니다.

사전 요구 사항

VMware Cloud Director 장치에서 FIPS 모드 활성화 또는 비활성화

절차

- 1 https://primary_eth1_ip_address:5480에서 장치 관리 UI에 **루트**로 로그인합니다.
- 2 왼쪽 패널에서 **시스템 구성**을 선택합니다.
- 3 각 노드에서 장치 및 셀 FIPS 모드의 상태를 봅니다.

VMware Cloud Director 장치 SNMP 에이전트 구성

VMware Cloud Director 10.2.2부터 VMware Cloud Director 장치 SNMP 에이전트가 폴링 요청을 수신 대기하도록 구성할 수 있습니다.

SNMP(Simple Network Management Protocol)는 네트워크 요소의 관리 및 모니터링을 위한 애플리케이션 계층 프로토콜입니다. VMware Cloud Director 장치에는 GET, GETBULK 및 GETNEXT 요청을 수신하고 응답할 수 있는 SNMP 에이전트가 포함되어 있습니다. VMware Cloud Director 장치 SNMP 에이전트는 SNMP 표준을 준수하는 모든 SNMP 관리 서비스와 호환됩니다. SNMP v1, v2c 또는 v3용 에이전트를 구성할 수 있습니다. 단, 암호화 인증 및 암호화를 비롯한 향상된 보안은 SNMP v3에서만 제공됩니다.

기존 Net-SNMP 에이전트가 있는 경우 구성을 시작하기 전에 다음을 고려하십시오.

- 버전 10.2.2 이상으로 업그레이드하는 동안 VMware Cloud Director는 Net-SNMP를 삭제하고 VMware-SNMP로 대체합니다.
- Net-SNMP에서 작동하는 기존 방화벽 규칙은 제거해야 합니다. VMware-SNMP는 snmpd 서비스를 시작 및 중지할 때 폴링 포트를 활성화 및 비활성화하기 때문입니다.

VMware Cloud Director 장치용 VMware-SNMP는 다음과 같은 표준 산업 MIB를 통해 사용할 수 있는 표준 Linux OS MIB(Management Information Base)를 지원합니다.

- SNMPv2-MIB
- RFC 3418IF-MIB
- RFC 2863IP-MIB
- RFC 4293IP-FORWARD-MIB
- RFC 4292UDP-MIB
- RFC 4113TCP-MIB
- RFC 4022ENTITY-MIB
- RFC 4133HOST-RESOURCES-MIB
- RFC 2790VMWARE-SYSTEM-MIB, REVISION 201008020000Z

SNMP 에이전트에 대한 사용자 지정 포트 구성

VMware Cloud Director 10.2.2부터 폴링을 위한 VMware Cloud Director SNMP 에이전트를 구성하는 경우 GET, GETNEXT 및 GETBULK 요청과 같은 SNMP 관리 클라이언트 시스템의 요청을 수신 대기하고 응답할 수 있습니다.

기본적으로, 내장된 SNMP 에이전트는 관리 시스템에서 보내는 폴링 요청을 UDP 포트 161에서 수신 대기합니다. `vicfg-snmp --port` 명령을 사용하여 대체 포트를 구성할 수 있습니다. SNMP 에이전트용 포트와 다른 서비스의 포트 간에 충돌을 방지하려면 <https://ports.vmware.com/home/VMware-Cloud-Director>의 내용을 참조하십시오.

사전 요구 사항

Net-SNMP에서 작동하는 기존 방화벽 규칙은 제거해야 합니다. VMware-SNMP는 `snmpd` 서비스를 시작 및 중지할 때 폴링 포트를 활성화 및 비활성화하기 때문입니다.

절차

- 1 관리 권한이 있는 사용자로 장치 셸에 로그인합니다.
- 2 다음 명령을 실행하여 SNMP를 비활성화합니다.

```
vicfg-snmp --disable
```

- 3 SNMP 에이전트가 폴링 요청을 수신 대기하는 데 사용하는 포트를 변경하려면 다음 명령을 실행합니다.

```
vicfg-snmp --port port_number
```


SNMP v1 및 v2c용 VMware Cloud Director 장치 구성

VMware Cloud Director 10.2.2부터 SNMP 에이전트에 대해 하나 이상의 커뮤니티를 구성하여 SNMP용 VMware Cloud Director 장치를 구성할 수 있습니다. SNMP v1 및 v2c용 VMware Cloud Director SNMP 에이전트를 구성하면 에이전트가 폴링을 지원합니다.

SNMP v1 및 v2c에서 커뮤니티 문자열은 하나 이상의 관리되는 개체가 포함된 네임스페이스입니다. 네임스페이스는 인증을 위한 하나의 형태로 작동할 수 있지만 통신을 보호하지는 않습니다. 통신을 보호하려면 SNMP v3을 사용합니다.

VMware Cloud Director 장치 SNMP 에이전트에서 SNMP v1 및 v2c 메시지를 보내고 받을 수 있도록 하려면 에이전트에 대해 하나 이상의 커뮤니티를 구성해야 합니다. SNMP 커뮤니티는 디바이스 및 관리 시스템의 그룹을 정의합니다. 동일한 커뮤니티의 멤버인 디바이스와 관리 시스템만 SNMP 메시지를 교환할 수 있습니다. 하나의 디바이스 또는 관리 시스템이 여러 커뮤니티의 멤버일 수 있습니다.

절차

- 1 관리 권한이 있는 사용자로 장치 셸에 로그인합니다.
- 2 SNMP 커뮤니티를 구성하기 위해 `vicfg-snmp -c` 명령을 실행합니다.

예를 들어 `public`, `east` 및 `west` 네트워크 운영 센터 커뮤니티를 구성하려면 다음 명령을 실행합니다.

```
vicfg-snmp --communities public,eastnoc,westnoc
```

이 명령으로 커뮤니티를 지정할 때마다 지정한 설정이 이전 구성을 덮어씁니다. 여러 커뮤니티를 입력하려면 쉼표를 구분 기호로 사용하십시오.

- 3 다음 명령을 실행하여 SNMP를 사용하도록 설정합니다.

```
vicfg-snmp --enable
```

SNMP v3용 VMware Cloud Director 장치 구성

VMware Cloud Director 10.2.2부터 SNMP v3용 VMware Cloud Director 장치를 구성할 수 있습니다. SNMP v3용 SNMP 에이전트를 구성하면 에이전트가 폴링을 지원하고 암호화 인증 및 암호화를 비롯한 보다 강력한 보안을 제공합니다.

SNMP v3용 VMware Cloud Director 장치 구성은 세 부분으로 구성됩니다.

- 1 SNMP 엔진 ID 구성
- 2 SNMP 인증 및 개인 정보 보호 프로토콜 구성
- 3 SNMP 사용자 구성

모든 SNMP v3 에이전트에는 에이전트의 고유 식별자 역할을 하는 엔진 ID가 있습니다. 엔진 ID는 해싱 함수와 함께 SNMP v3 메시지의 인증 및 암호화를 위한 지역화된 키를 생성하는 데 사용됩니다. SNMP 에이전트를 사용하도록 설정하기 전에 엔진 ID를 지정하지 않으면 독립형 SNMP 에이전트를 사용하도록 설정할 때 VMware Cloud Director에서 엔진 ID가 생성됩니다.

사용자의 ID 를 확인하기 위해 인증을 사용할 수 있습니다. 개인 정보 보호는 데이터의 기밀성을 보장하기 위해 **SNMP v3** 메시지 암호화를 허용합니다. 개인 정보 보호 프로토콜은 보안을 위해 커뮤니티 문자열을 사용하는 **SNMP v1** 및 **v2c**에서 사용할 수 있는 것보다 높은 수준의 보안을 제공합니다. 인증 및 개인 정보 보호는 모두 선택 사항입니다. 단, 개인 정보 보호를 사용하도록 설정하려면 인증을 사용하도록 설정해야 합니다.

인증 및 개인 정보 보호 프로토콜의 기본값은 없음입니다.

SNMP v3 정보에 액세스할 수 있는 사용자를 다섯 명까지 구성할 수 있습니다. 사용자 이름은 **32**자를 넘지 않아야 합니다. 사용자를 구성하는 동안 사용자의 인증 및 개인 정보 보호 암호와 **SNMP** 에이전트의 엔진 ID를 기반으로 인증 및 개인 정보 보호 해시 값을 생성합니다. 사용자를 구성한 후 엔진 ID, 인증 프로토콜 또는 개인 정보 보호 프로토콜을 변경하면 사용자가 무효화되므로 재구성해야 합니다.

사전 요구 사항

SNMP 인증 및 개인 정보 보호 프로토콜을 구성하려면 구성하려는 각 사용자의 인증 및 개인 정보 보호 암호를 알고 있어야 합니다. 암호는 **8**자 이상이어야 합니다.

절차

- 1 관리 권한이 있는 사용자로 장치 셸에 로그인합니다.
- 2 `vicfg-snmp --engineid` 명령을 실행하여 대상을 구성합니다.

예를 들어 다음 명령을 실행합니다.

```
vicfg-snmp --engineid 80001f8880167b18238d613d6000000000
```

여기서 **80001f8880167b18238d613d6000000000**은 ID이며, 5~32자 길이의 16진수 문자열이어야 합니다.

- 3 (선택 사항) 인증 프로토콜을 구성하기 위해 `vicfg-snmp --authentication` 명령을 실행합니다.

예를 들어 다음 명령을 실행합니다.

```
vicfg-snmp --authentication protocol
```

여기서 *protocol*은 **none**(인증을 사용하지 않을 경우), **SHA1**, **SHA256**, **SHA384** 또는 **SHA512**여야 합니다. 예를 들어 인증 프로토콜을 **SHA512**로 설정하려면 다음 명령을 실행해야 합니다.

```
vicfg-snmp --authentication SHA512
```

- 4 (선택 사항) 개인 정보 보호 프로토콜을 구성하기 위해 `vicfg-snmp --privacy` 명령을 실행합니다.

예를 들어 다음 명령을 실행합니다.

```
vicfg-snmp --privacy protocol
```

여기서 *protocol*은 **none**(개인 정보 보호를 사용하지 않을 경우), **AES128**, **AES192** 또는 **AES256**이어야 합니다. 예를 들어 개인 정보 보호 프로토콜을 **AES128**로 설정하려면 다음 명령을 실행해야 합니다.

```
vicfg-snmp --privacy AES128
```

- 5 인증, 개인 정보 보호 또는 둘 다를 사용하여 사용자에게 대한 인증 및 개인 정보 보호 해시 값을 생성하는 경우 다음 명령을 실행합니다.

```
vicfg-snmp --hashkey authentication-password privacy-password
```

인증 및 개인 정보 보호 설정에 따라 *authentication-password*, *privacy-password* 또는 둘 다를 입력해야 합니다. 암호는 8자 이상이어야 합니다. *authentication-password* 및 *privacy-password*를 기록해 둡니다. SNMP 클라이언트를 설정하는 데 필요하기 때문입니다. 명령의 출력에는 인증 지역화된 키 및 개인 정보 보호 지역화된 키 정보가 포함됩니다.

- 6 다음 명령을 실행하여 사용자를 한 명 이상 구성합니다.

쉼표로 구분된 목록으로 추가하면 여러 사용자를 지정할 수 있습니다. 사용자는 최대 5명까지 구성할 수 있습니다.

```
vicfg-snmp --users userid/authhash/privhash/security
```

명령의 매개 변수는 다음과 같습니다.

매개 변수	설명
<i>userid</i>	사용자 이름으로 바꿉니다.
<i>authhash</i>	인증 지역화된 키로 바꿉니다.
<i>privhash</i>	개인 정보 보호 지역화된 키로 바꿉니다.
<i>model</i>	해당 사용자에게 대해 설정된 보안 수준, 즉 auth (인증만 사용할 경우), priv (인증과 개인 정보 보호를 사용할 경우) 또는 none (인증 또는 개인 정보 보호를 사용하지 않을 경우)으로 바꿉니다.

예를 들어 보안 없이 사용자를 구성하려면 다음을 실행하면 됩니다.

```
vicfg-snmp --users vcd-snmp-user/-/-/none
```

권한 부여 해시로 사용자를 구성하려면 다음을 실행하면 됩니다.

```
vicfg-snmp --users vcd-snmp-user/225e07958d3c6af615588db17d61986e69fb7a71/-/auth
```

권한 부여 해시 및 개인 정보 보호 해시를 사용하여 사용자를 구성하려면 다음을 실행하면 됩니다.

```
vicfg-snmp --users vcd-snmp-user/225e07958d3c6af615588db17d61986e69fb7a71/  
da1057af05f67a25a09265a9a2bedb53/priv
```

- 7 (선택 사항) 한 명 이상의 사용자를 삭제하려면 새 사용자 세부 정보로 6단계를 반복합니다.

*vicfg-snmp --users*를 다시 실행하면 이전 설정이 재정의됩니다.

8 다음 명령을 실행하여 SNMP를 사용하도록 설정합니다.

```
vicfg-snmp --enable
```

VMware Cloud Director SNMP에 snmpwalk 사용

VMware Cloud Director 10.2.2부터 하위 트리 내의 각 OID 또는 노드에 대해 고유한 명령을 입력하지 않고 GETNEXT 요청을 연결하려면 snmpwalk 명령을 실행하면 됩니다.

사전 요구 사항

- **SNMP v1 및 v2c용 VMware Cloud Director 장치 구성** 또는 **SNMP v3용 VMware Cloud Director 장치 구성**용 VMware Cloud Director 장치를 구성합니다.

절차

- 1 로컬 시스템에 snmpwalk 명령이 설치되어 있는지 확인하고 필요한 경우 설치합니다.
- 2 snmpwalk 명령을 실행합니다.

```
snmpwalk -v SNMP_version -l security_level -a authorization_protocol -A
authorization_password -x privacy_protocol -X privacy_password -u username host_IP:port
queried_MIB_OID
```

여기서 -l은 보안 수준이며 noAuthNoPriv, authNoPriv 또는 authPriv로 설정할 수 있습니다. snmpwalk 명령에 대한 도움말을 보려면 -h를 실행하면 됩니다.

예제: snmpwalk 쿼리

sysDescr.0 MIB OID의 샘플 쿼리는 다음과 같습니다.

```
snmpwalk -v 3 -l authPriv -a SHA512 -A myauthpassword -x AES128 -X myprivpassword -u vcd-snmp-
user 192.168.100.187:10161 sysDescr.0
```

이 명령은 다음 출력을 반환합니다.

```
SNMPv2-MIB::sysDescr.0 = STRING: VMware-Cloud-Director-Appliance 10.2.2.5553 generic build
17709283 VMware, Inc x86_64
```

VMware Cloud Director 장치 SNMP 설정 재설정

VMware Cloud Director 10.2.2부터는 VMware Cloud Director 장치 SNMP 에이전트를 구성할 수 있습니다. 모든 SNMP 설정을 지우고 에이전트를 비활성화하려면 장치 SNMP 설정을 재설정합니다.

사전 요구 사항

SNMP v1 및 v2c용 VMware Cloud Director 장치 구성 또는 **SNMP v3용 VMware Cloud Director 장치 구성**용 VMware Cloud Director 장치를 구성합니다.

절차

- 1 관리 권한이 있는 사용자로 장치 셸에 로그인합니다.

- 2 모든 SNMP 설정을 기본값으로 되돌리고 SNMP 에이전트를 비활성화하려면 다음 명령을 실행합니다.

```
vicfg-snmp --reset
```

VMware Cloud Director 장치 SNMP 설정 표시

VMware Cloud Director 10.2.2부터는 SNMP 설정(예: UDP 포트, 커뮤니티, V3 사용자, 엔진 ID, 권한 부여 및 개인 정보 보호 프로토콜 등)을 표시할 수 있습니다.

사전 요구 사항

SNMP v1 및 v2c용 VMware Cloud Director 장치 구성 또는 SNMP v3용 VMware Cloud Director 장치 구성용 VMware Cloud Director 장치를 구성합니다.

절차

- 1 관리 권한이 있는 사용자로 장치 셸에 로그인합니다.
- 2 SNMP 설정을 표시하려면 다음 명령을 실행합니다.

```
vicfg-snmp --show
```

예제: 샘플 vicfg-snmp --show 출력

샘플 출력은 권한 부여 해시 및 개인 정보 보호 해시가 있는 V3 사용자에 대해 SNMP 에이전트를 사용하도록 설정되어 있는 것을 보여줍니다.

```
Current SNMP agent setting
Enabled : true
UDP port : 161
V1/V2c Communities :
V1 Notification targets :
Notification filter oids:
V3 Notification targets :
V3 Users : vcd-snmp-user 225e07958d3c6af615588db17d61986e69fb7a71
da1057af05f67a25a09265a9a2bedb53 authPriv
Contact :
Location :
Engine ID : 80001f8880efbab0540a653e6000000000
Auth Protocol : usmHMACSHAAuthProtocol
Priv Protocol : usmAESCfb128PrivProtocol
Log level : warning
Process ID : 15828
Large Storage Support : False
Simple Application Names: False
INFO: listing complete.
```

VMware Cloud Director 장치의 DNS 설정 편집

배포 후에 VMware Cloud Director 장치의 DNS 서버를 하나 이상 변경할 수 있습니다.

중요 장치의 호스트 이름은 편집할 수 없습니다. 원하는 호스트 이름을 사용하여 새 장치를 배포해야 합니다.

사전 요구 사항

OVF 속성을 영구적으로 변경하려면 vSphere UI를 사용하여 OVF 속성 값을 변경해야 합니다. "vSphere 가상 시스템 관리" 가이드에서 vApp 속성 구성 항목을 참조하십시오.

절차

- 1 예를 들어 테스트 목적으로 DNS 설정을 일시적으로 변경하려면 VMware Cloud Director에서 DNS 설정을 편집합니다.

- a VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- b (선택 사항) 다음 명령을 실행하여 현재 DNS 구성을 확인합니다.

```
ovfenv --key vami.DNS.VMware_vCloud_Director
```

- c DNS 서버를 하나 이상 변경합니다.

여러 DNS 서버를 지정하려면, *DNS_server_IP*를 공백 없이 쉼표로 구분된 목록으로 설정합니다.

```
ovfenv --key vami.DNS.VMware_vCloud_Director --value DNS_server_IP
```

- d 변경 내용을 적용하려면 VAOS 서비스를 다시 시작합니다.

```
systemctl restart vaos.service
```

- 2 DNS 설정을 영구적으로 변경하려는 경우에는 vSphere UI를 사용하여 *vami.DNS.VMware_vCloud_Director* 속성의 값을 새 DNS 서버 IP 주소로 설정합니다.

여러 DNS 서버를 지정하려면 공백 없이 쉼표로 구분된 목록을 입력합니다.

참고 vSphere의 속성 값을 변경하려면 VM의 전원을 꺼야 합니다.

VMware Cloud Director 장치 네트워크 인터페이스에 대한 정적 경로 편집

초기 VMware Cloud Director 배포 후에 eth0 및 eth1 네트워크 인터페이스에 대한 정적 경로를 변경할 수 있습니다.

사전 요구 사항

OVF 속성을 영구적으로 변경하려면 vSphere UI를 사용하여 OVF 속성 값을 변경해야 합니다. "vSphere 가상 시스템 관리" 가이드에서 vApp 속성 구성 항목을 참조하십시오.

절차

- 1 예를 들어 테스트 목적으로 정적 경로 값을 일시적으로 변경하려면 VMware Cloud Director에서 정적 경로를 편집합니다.

- a VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.

- b (선택 사항) 현재 정적 경로 구성을 확인합니다.

- eth0에 대해 다음 명령을 실행합니다.

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director
```

- eth1에 대해 다음 명령을 실행합니다.

```
ovfenv --key vcloudnet.routes1.VMware_vCloud_Director
```

- c 정적 경로 값을 변경합니다.

정적 경로는 쉼표로 구분된 경로 규격 목록에 있어야 합니다. 예를 들어 eth0에 대해 다음을 실행해야 합니다.

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director --value "172.16.100.253  
172.16.96.0/19, 172.16.100.253 192.168.100.0/24"
```

- eth0에 대해 다음 명령을 실행합니다.

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director --value "new_static_routes0"
```

- eth1에 대해 다음 명령을 실행합니다.

```
ovfenv --key vcloudnet.routes1.VMware_vCloud_Director --value "new_static_routes1"
```

- d VMware Cloud Director 장치에서 네트워크 서비스를 다시 시작합니다.

```
systemctl restart vcd-ova-netconfig.service
```

- 2 정적 경로 값을 영구적으로 변경하려는 경우에는 vSphere UI를 사용하여 OVF 속성을 변경합니다.

정적 경로는 쉼표로 구분된 경로 규격 목록에 있어야 합니다.

참고 vSphere의 속성 값을 변경하려면 VM의 전원을 꺼야 합니다.

- vSphere 사용자 인터페이스를 사용하여 vcloudnet.routes0.VMware_vCloud_Director 속성의 값을 새 경로 규격 문자열로 설정합니다.
- vSphere 사용자 인터페이스를 사용하여 vcloudnet.routes1.VMware_vCloud_Director 속성의 값을 새 경로 규격 문자열로 설정합니다.

VMware Cloud Director 장치의 구성 스크립트

VMware Cloud Director 장치에는 특정 구성 스크립트가 포함되어 있습니다.

디렉터리	설명
/opt/vmware/appliance/bin/	장치 구성 스크립트.
/opt/vmware/appliance/etc/	장치 구성 파일.
/opt/vmware/appliance/etc/pg_hba.d/	pg_hba.conf 파일에 사용자 지정 항목을 추가할 수 있는 디렉토리. VMware Cloud Director 데이터베이스에 대한 외부 액세스 구성 의 내용을 참조하십시오.

VMware Cloud Director 장치 인증서 갱신

VMware Cloud Director 장치를 배포하면 유효 기간이 365일인 자체 서명된 인증서가 생성됩니다. 환경에 만료될 예정이거나 만료된 인증서가 있는 경우 자체 서명 인증서를 새로 생성할 수 있습니다. 각 VMware Cloud Director 셀에 대한 인증서를 개별적으로 갱신해야 합니다.

VMware Cloud Director 장치는 2개의 SSL 인증서 집합을 사용합니다. VMware Cloud Director 서비스는 HTTPS 및 콘솔 프록시 통신을 위해 하나의 인증서 집합을 사용합니다. 내장된 PostgreSQL 데이터베이스와 VMware Cloud Director 장치 관리 사용자 인터페이스는 다른 SSL 인증서 집합을 공유합니다.

자체 서명된 인증서 집합을 둘 다 변경할 수 있습니다. 또는 VMware Cloud Director의 HTTPS 및 콘솔 프록시 통신에 CA 서명된 인증서를 사용하는 경우에는 내장형 PostgreSQL 데이터베이스 및 장치 관리 UI 인증서만 변경할 수 있습니다. CA 서명된 인증서에는 잘 알려진 공용 인증 기관에 근거한 완전 신뢰 체인이 포함됩니다.

사전 요구 사항

- 데이터베이스 고가용성 클러스터에서 기본 노드에 대한 인증서를 갱신하는 경우 데이터 손실을 방지하기 위해 다른 모든 노드를 유지 보수 모드로 지정합니다. [셀 관리](#)를 참조하십시오.
- FIPS 모드를 사용하도록 설정한 경우 장치의 **루트** 암호는 14자 이상을 포함해야 합니다. [VMware Cloud Director 장치 루트 암호 변경](#)의 내용을 참조하십시오.

절차

- 1 VMware Cloud Director 장치의 OS에 **root**로 직접 로그인하거나 SSH를 통해 연결합니다.
- 2 VMware Cloud Director 서비스를 중지하려면 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u administrator cell --shutdown
```


3 데이터베이스 및 장치 관리 UI 또는 HTTPS 및 콘솔 프록시 통신, 데이터베이스 및 장치 관리 UI에 대해 자체 서명된 인증서를 새로 생성합니다.

- 내장형 PostgreSQL 데이터베이스 및 VMware Cloud Director 장치 관리 UI에 대해서만 자체 서명된 인증서를 생성합니다. 다음을 실행합니다.

```
/opt/vmware/appliance/bin/generate-certificates.sh <root-password> --skip-vcd-certs
```

이 명령은 내장된 PostgreSQL 데이터베이스 및 장치 관리 UI에 대해 새로 생성된 인증서를 자동으로 사용합니다. PostgreSQL 및 Nginx 서버가 다시 시작됩니다.

- 내장형 PostgreSQL 데이터베이스 및 장치 관리 UI에 대한 인증서에 더하여 VMware Cloud Director의 HTTPS 및 콘솔 프록시 통신을 위한 자체 서명된 인증서를 생성합니다.

a 다음 명령을 실행합니다.

```
/opt/vmware/appliance/bin/generate-certificates.sh <root-password>
```

- b CA 서명된 인증서를 사용하지 않는 경우 명령을 실행하여 새로 생성한 자체 서명된 인증서를 VMware Cloud Director로 가져옵니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --  
keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password <root-  
password>
```

- c VMware Cloud Director 서비스를 다시 시작합니다.

```
service vmware-vcd start
```

이 명령은 내장된 PostgreSQL 데이터베이스 및 장치 관리 UI에 대해 새로 생성된 인증서를 자동으로 사용합니다. PostgreSQL 및 Nginx 서버가 다시 시작됩니다. 이 명령은 VMware Cloud Director의 HTTPS 및 콘솔 프록시 통신을 위한 자체 서명된 새 인증서(4에서 사용됨)를 사용하여 새로운 인증서 키 저장소(/opt/vmware/vcloud-director/certificates.ks)를 생성합니다.

결과

갱신된 자체 서명 인증서가 VMware Cloud Director 사용자 인터페이스에 표시됩니다.

다음 번에 appliance-sync 함수가 실행될 때 다른 VMware Cloud Director 셀의 VMware Cloud Director truststore로 새 PostgreSQL 인증서를 가져옵니다. 이 작업에는 최대 60초가 걸릴 수 있습니다.

다음에 수행할 작업

필요한 경우 자체 서명된 인증서를 외부 또는 내부 CA(인증 기관)에서 서명한 인증서로 교체할 수 있습니다.

자체 서명된 내장형 PostgreSQL 및 VMware Cloud Director 장치 관리 UI 인증서 교체

기본적으로 내장형 PostgreSQL 데이터베이스 및 VMware Cloud Director 장치 관리 사용자 인터페이스는 자체 서명된 SSL 인증서 집합을 공유합니다. 보안 강화를 위해 자체 서명된 기본 인증서를 CA(인증 기관) 서명 인증서로 교체할 수 있습니다.

VMware Cloud Director 장치를 배포하면 유효 기간이 365일인 자체 서명된 인증서가 생성됩니다. VMware Cloud Director 장치는 2개의 SSL 인증서 집합을 사용합니다. VMware Cloud Director 서비스는 HTTPS 및 콘솔 프록시 통신에 대해 하나의 인증서 집합을 사용합니다. 내장된 PostgreSQL 데이터베이스와 VMware Cloud Director 장치 관리 사용자 인터페이스는 다른 SSL 인증서 집합을 공유합니다.

참고 데이터베이스 및 장치 관리 UI 인증서를 교체하는 프로세스는 HTTPS 및 콘솔 프록시 통신에 대한 인증서에 영향을 주지 않습니다. 인증서 집합 중 하나를 교체한다고 해서 다른 집합을 교체해야 하는 것은 아닙니다.

절차

- 1 서명을 위해 /opt/vmware/appliance/etc/ssl/vcd_ova.csr에 있는 인증서 서명 요청을 CA에 전송합니다.
- 2 기본 데이터베이스의 인증서를 교체하는 경우 데이터 손실 가능성을 막기 위해 다른 모든 노드를 유지 보수 모드로 전환합니다.
- 3 /opt/vmware/appliance/etc/ssl/vcd_ova.crt에 있는 기존 PEM 형식 인증서를 1단계에서 CA로부터 확보한 서명된 인증서로 바꿉니다.
- 4 새 인증서를 선택하려면 vpostgres, nginx 및 vcd_ova_ui 서비스를 다시 시작합니다.

```
systemctl restart nginx.service && systemctl restart vcd_ova_ui.service
```

```
systemctl restart vpostgres.service
```

- 5 기본 데이터베이스에 대한 인증서를 교체하는 경우 다른 모든 노드를 유지 보수 모드에서 해제합니다.

결과

다음에 appliance-sync 함수가 실행될 때 다른 VMware Cloud Director 셀의 VMware Cloud Director truststore로 새 인증서를 가져옵니다. 이 작업에는 최대 60초가 걸릴 수 있습니다.

VMware Cloud Director 장치를 위한 전송 서버 스토리지 바꾸기

배포 후에 VMware Cloud Director 장치에 대한 NFS 공유를 변경할 수 있습니다.

절차

- 1 VMware Cloud Director 서버 그룹의 모든 장치에서 vmware-vcd 서비스를 정지시키고 중지합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u admin_username cell --shutdown
```

- 2 서버 그룹의 모든 장치에서 `appliance-sync.timer` 서비스를 중지합니다.

```
systemctl stop appliance-sync.timer
```

- 3 기본 장치에서 이전 NFS 공유의 데이터를 새 NFS 공유로 복사합니다.

- a 새 NFS 공유 마운트 지점을 만듭니다.

```
mkdir /opt/vmware/vcloud-director/data/transfer-new/
```

- b 새 마운트 지점에 새 NFS 서버 공유를 마운트합니다.

```
mount -t nfs Primary_appliance_IP_address:/data/transfer /opt/vmware/vcloud-director/
data/transfer-new
```

- c 이전 전송 공유의 파일을 새 전송 공유로 복사합니다.

참고 파일을 복사하는 데 걸리는 시간은 전송 폴더 공유에 캐시된 카탈로그 항목의 수에 따라 다릅니다.

```
cp -R /opt/vmware/vcloud-director/data/transfer/* /opt/vmware/vcloud-director/data/
transfer-new/
```

- d 파일 복사가 완료되면 `/opt/vmware/vcloud-director/data/transfer-new`의 콘텐츠를 확인하거나 다음 명령을 실행하여 이전 NFS 공유의 콘텐츠가 새 NFS 공유에 있는지 확인합니다.

```
diff -r --brief /opt/vmware/vcloud-director/data/transfer/ /opt/vmware/vcloud-director/
data/transfer-new/
```

- e 임시 마운트 지점에서 새 NFS 공유를 마운트 해제합니다.

```
umount /opt/vmware/vcloud-director/data/transfer-new/
```

- f 임시 마운트 지점을 삭제합니다.

```
rmdir /opt/vmware/vcloud-director/data/transfer-new/
```

- 4 NFS 줄을 새 NFS 서버의 경로로 대체하여 `/etc/fstab` 파일을 업데이트합니다.

```
Primary_appliance_IP_address:/data/transfer_appliance /opt/vmware/vcloud-director/data/
transfer/ nfs defaults 0 0
```

- 5 이전 NFS 공유를 마운트 해제합니다.

```
umount /opt/vmware/vcloud-director/data/transfer/
```

- 6 새 NFS 공유를 마운트합니다.

```
mount -a
```

- 7 mount 명령의 출력에 마운트된 NFS 공유가 나열되는지 확인하여 NFS 공유를 성공적으로 마운트했는지 확인합니다.
- 8 다음 명령을 사용하여 전송 디렉토리의 소유권을 root에서 vcloud로 변경합니다.

```
chown -R vcloud:vcloud /opt/vmware/vcloud-director/data/transfer
```

- 9 appliance-sync.timer 서비스를 다시 시작합니다.

```
systemctl start appliance-sync.timer
```

- 10 서버 그룹의 모든 노드에서 4~9단계를 반복합니다.
- 11 한 번에 노드 하나씩 vmware-vcd 서비스를 다시 시작합니다.

```
systemctl start vmware-vcd
```

- 12 서버 그룹의 모든 노드에서 vmware-vcd가 올바르게 작동하는지 확인합니다.

VMware Cloud Director 장치에서 내장형 PostgreSQL 데이터베이스의 용량 늘리기

VMware Cloud Director 장치의 PostgreSQL 데이터베이스 디스크에 공간이 부족한 경우에는 내장형 PostgreSQL 데이터베이스의 용량을 늘릴 수 있습니다.

PostgreSQL 데이터베이스는 하드 디스크 3에 상주합니다. 기본 크기는 80GB입니다. 이 절차는 장치가 작동하는 동안 수행할 수 있습니다.

중요 기본 장치의 용량을 늘리기 전에 기존 대기 장치의 용량을 늘려야 합니다.

각 대기 장치의 PostgreSQL 데이터베이스 디스크 크기는 기본 장치의 PostgreSQL 데이터베이스 디스크와 동일해야 합니다.

사전 요구 사항

- VMware Cloud Director 환경에 대기 노드가 있으면, 대기 노드와 기본 노드를 식별하고 대기 노드에서 절차를 시작합니다. 노드의 역할 식별에 대한 자세한 내용은 [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.
- VMware Cloud Director 환경이 기본 노드로만 구성된 경우에는 기본 노드에서 절차를 실행합니다.

절차

- 1 하드 디스크 3의 용량을 원하는 크기로 늘리려면 vSphere Client에 로그인합니다.

각 대기 장치의 PostgreSQL 데이터베이스 디스크 크기는 기본 장치의 PostgreSQL 데이터베이스 디스크만큼 커야 합니다.

- a 변경할 장치 가상 시스템을 선택합니다.
- b **작업 > 설정 편집**을 선택합니다.
- c **하드 디스크 3**의 크기를 늘리고 **확인**을 클릭합니다.

재구성 작업의 진행률이 **최근 작업** 창에 나타납니다.

- 2 장치 노드의 OS에 변경 내용을 적용합니다.

- a VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- b 하드 디스크 크기 조정 변경 내용을 OS에 적용하려면 다음 스크립트를 실행합니다.

```
/opt/vmware/appliance/bin/db_diskresize.sh
```

- 3 환경이 하나의 기본 장치로만 구성되어 있지 않으면 데이터베이스가 있는 각 노드에 대해 절차를 반복합니다.

VMware Cloud Director 장치에서 PostgreSQL 구성 수정

PostgreSQL ALTER SYSTEM 명령을 사용하여 VMware Cloud Director 장치 PostgreSQL 구성을 변경할 수 있습니다.

ALTER SYSTEM 명령은 매개 변수 설정의 변경 사항을 postgresql.auto.conf 파일에 기록하며, 이것은 PostgreSQL 초기화 중에 postgresql.conf 파일보다 우선합니다. 일부 설정은 PostgreSQL 서비스를 다시 시작해야 하지만 다른 설정은 동적으로 구성되며 다시 시작할 필요가 없습니다.

postgresql.conf 파일을 변경하지 마십시오. 클러스터 작업을 위해서는 파일을 주기적으로 덮어써야 하며 변경 사항이 지속되지 않기 때문입니다.

절차

- 1 기본 장치의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 사용자를 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

- 3 PostgreSQL ALTER SYSTEM 명령을 사용하여 매개 변수를 변경합니다.

```
psql -c "ALTER SYSTEM set 매개 변수='값';"
```

- 4 변경하려는 각 구성 매개 변수에 대해 단계 3을 반복합니다.

- 5 변경하려는 매개 변수 중 일부가 PostgreSQL 서비스를 다시 시작해야 하는 경우 `vpostgres` 프로세스를 다시 시작합니다.

```
systemctl restart vpostgres
```

- 6 환경에 대기 노드가 있는 경우 `postgresql.auto.conf` 파일을 대기 장치에 복사하고 필요한 경우 PostgreSQL 서비스를 다시 시작합니다.

- a 기본 노드에서 대기 노드로 `postgresql.auto.conf`를 복사합니다.

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
```

- b 복사된 `postgresql.auto.conf` 파일의 매개 변수 중 일부가 다시 시작해야 적용되는 경우 대기 노드에서 `vpostgres` 프로세스를 다시 시작합니다.

```
systemctl restart vpostgres
```

- c 각 대기 노드에 대해 6.a 및 6.b를 반복합니다.

데이터베이스 고가용성 클러스터에서 실행 중인 대기 셀 등록 취소

노드를 다른 역할로 사용하려는 경우나 고가용성 클러스터에서 노드를 제거하려는 경우에는 등록을 취소해야 합니다.

VMware Cloud Director 장치 API에 대한 자세한 내용은 [VMware Cloud Director 장치 API](#) 설명서를 참조하십시오.

정상적인 시스템 작동 중에 셀 등록을 취소할 수 있습니다.

참고 기본 노드가 정상적으로 작동하려면 하나 이상의 대기 노드가 항상 실행 중이어야 합니다.

절차

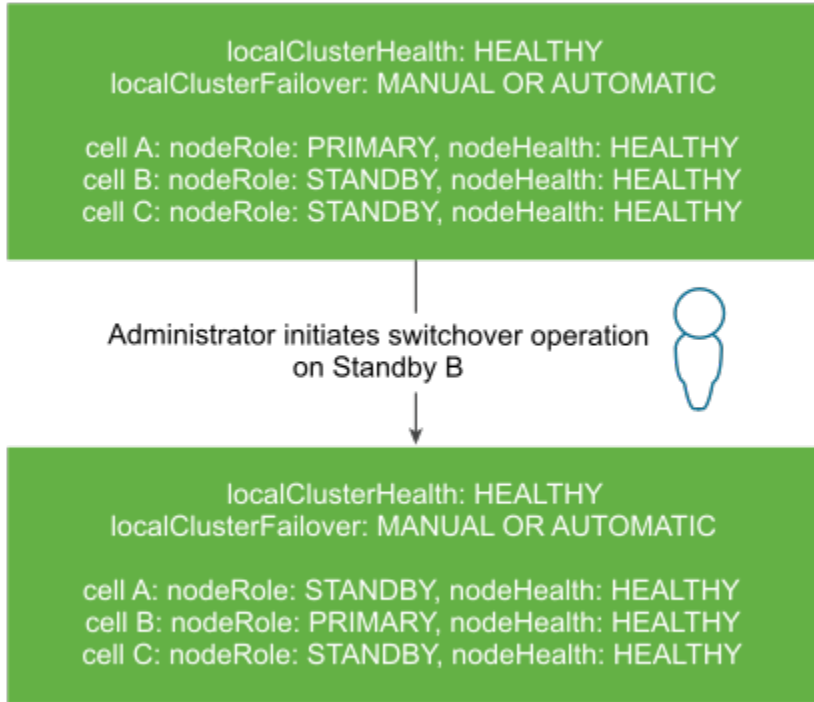
- 1 등록을 취소하려는 대기 노드의 이름을 찾기 위해 VMware Cloud Director 장치 API 메서드 `NODES`를 실행합니다.
- 2 다른 노드 중 하나에서 VMware Cloud Director 장치 API 메서드 `UNREGISTER`를 실행합니다.
여기서 `node-name`은 제거하려는 대기 장치의 이름입니다.
- 3 등록이 취소된 대기 노드가 데이터베이스 고가용성 클러스터에 더 이상 나타나지 않는지 확인하기 위해 API 메서드 `NODES`를 실행합니다.

데이터베이스 고가용성 클러스터에서 기본 및 대기 셀의 역할 전환

VMware Cloud Director 장치의 관리 UI를 사용하여 데이터베이스 고가용성 클러스터에서 셀의 역할을 전환하고 다른 셀을 기본으로 승격할 수 있습니다.

VMware Cloud Director 장치 관리 사용자 인터페이스 또는 VMware Cloud Director 장치 API를 사용하여 기본 및 대기 셀의 역할을 전환할 수 있습니다. 이 절차에서는 관리 UI를 사용하여 전환 작업을 수행하는 단계를 설명합니다.

그림 3-3. 기본 및 대기 셀 간 전환



사전 요구 사항

- 클러스터의 모든 노드가 정상이고 온라인 상태인지 확인합니다. [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.

절차

- 서버 그룹의 일부인 모든 VMware Cloud Director 셀에서 활동을 중지하거나 셀을 유지 보수 모드로 전환합니다.
이 전환으로 인해 30 – 60초 동안 VMware Cloud Director 데이터베이스를 사용할 수 없게 됩니다. 예기치 않은 작업 실패를 방지하려면 클러스터의 모든 셀에서 작업을 중지해야 합니다.
- https://primary_eth1_ip_address:5480에서 장치 관리 UI에 **루트**로 로그인합니다.
- 왼쪽 패널에서 **내장형 데이터베이스 가용성**을 선택합니다.
셀의 이름, 해당 역할과 상태, 대기 셀이 따르는 셀의 이름을 볼 수 있습니다.
- 클러스터 상태가 Healthy인지 확인합니다.
- 기본으로 승격하려는 셀에 대해 **전환** 버튼을 클릭하고 전환을 확인합니다.

- 6 전환 작업이 완료되면 스케줄러를 다시 시작하거나 클러스터의 셀에 대해 유지 보수 모드를 비활성화합니다.

MQTT 클라이언트를 사용하여 이벤트, 작업 및 메트릭 구독

MQTT 클라이언트를 사용하여 VMware Cloud Director 이벤트 및 작업에 대한 메시지를 구독할 수 있습니다.

MQTT는 경량, 바이너리, 메시징 전송 프로토콜입니다. VMware Cloud Director는 MQTT를 사용하여 이벤트 및 작업에 대한 정보를 게시하며, 사용자는 MQTT 클라이언트를 사용하여 메시지를 구독할 수 있습니다. MQTT 메시지는 MQTT 브로커를 통과하며, 이 브로커는 클라이언트가 온라인 상태가 아닌 경우에도 메시지를 저장할 수 있습니다.

VMware Cloud Director 10.2.2부터는 MQTT 클라이언트를 사용하여 메트릭을 구독할 수 있습니다.

사전 요구 사항

- WebSocket을 지원하는 MQTT 클라이언트가 있는지 확인합니다.
- WebSocket 업그레이드된 요청에 헤더를 추가할 수 있는지 확인합니다.
- 메트릭을 구독하려면 메트릭 수집을 구성하고 메트릭 게시를 사용하도록 설정합니다. [메트릭 수집 및 게시 구성](#)의 내용을 참조하십시오.

절차

- 1 OpenAPI 끝점을 사용하여 VMware Cloud Director에 로그인합니다.
- 2 WebSocket 연결을 설정하려면 Sec-WebSocket-Protocol 속성을 mqtt로 설정하고, 클라이언트를 /messaging/mqtt 경로에 연결하도록 설정하고, 인증 헤더를 추가하고, 표준 MQTT 연결 흐름을 따릅니다.

VMware Cloud Director에 대한 표준 로그인 요청에서 JWT 토큰을 수신합니다. 사용자 이름과 암호는 비워 둘 수 있습니다.

```
Sec-WebSocket-Protocol: mqtt
```

```
Authorization: Bearer {JWT_token}
```

- 3 연결이 성공적으로 설정되면 MQTT 클라이언트를 통해 항목을 구독합니다.

```
publish/{user_org_id}/{user_id}
```

```
publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
```

조직 관리자는 와일드카드를 사용하여 모든 조직 항목에 액세스할 수 있습니다.

```
publish/{user_org_id}/+
```


시스템 관리자는 와일드카드를 사용하여 모든 항목에 액세스할 수 있습니다.

```
publish/#
```

- 4 (선택 사항) VMware Cloud Director 10.2.2 이상인 경우 메트릭을 구독합니다.

```
metrics/{org_id}/{vApp_id}
```

시스템 관리자만 메트릭 항목에 액세스할 수 있습니다.

자동 스케일 그룹

VMware Cloud Director 10.2.2부터는 현재 CPU 및 메모리 사용에 따라 테넌트 사용자가 애플리케이션을 자동 스케일링하도록 허용할 수 있습니다.

CPU 및 메모리 사용에 대해 미리 정의한 조건에 따라, 테넌트는 VMware Cloud Director를 사용하여 선택한 스케일 그룹의 VM 수를 자동으로 스케일 업/다운할 수 있습니다. 테넌트가 애플리케이션을 자동으로 스케일링하도록 허용하려면 자동 스케일 솔루션에 대한 액세스 권한을 구성, 게시 및 부여해야 합니다.

동일한 애플리케이션을 실행하도록 구성된 서버에 대해 로드 밸런싱을 수행하려면 VMware NSX Advanced Load Balancer(Avi Networks)를 사용하면 됩니다.

자동 스케일 플러그인 구성 및 게시

테넌트에 대한 액세스 권한을 부여하기 전에 자동 스케일 그룹 솔루션을 구성해야 합니다. 자동 스케일링은 VMware Cloud Director 10.2.2부터 사용할 수 있습니다.

- 클러스터에 있는 셀의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- Cassandra 데이터베이스에서 메트릭 수집을 설정하여 메트릭 데이터 수집을 사용하도록 설정하거나 메트릭 데이터 지속성 없이 메트릭을 수집합니다.

- **기간별 메트릭 데이터 저장**을 위한 [Cassandra 데이터베이스 설치 및 구성](#)
- 데이터 지속성 없이 메트릭 데이터를 수집하려면 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.collect.only -v true
```

- 3 메트릭 게시를 사용하도록 설정합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

- 4 /tmp 폴더에 다음 내용으로 metrics.groovy 파일을 생성합니다.

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
```

```

        instance=""
        minReportingInterval=300
        aggregator="AVERAGE"
    }
}

```

- 5 파일을 가져옵니다.

```

$VCLLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
metrics.groovy

```

- 6 이전에 Cassandra를 구성한 경우 올바른 노드 주소, 데이터베이스 인증 세부 정보, 포트 및 메트릭 TTL(Time to Live)(일)을 제공하여 Cassandra 스키마를 업데이트합니다.

```

$VCLLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -
ttl TTL_days -update-schema

```

- 7 CA 서명된 인증서를 사용하여 셀을 실행하는 경우 자동 스케일링을 사용하도록 설정하려면 다음 명령을 실행합니다.

```

$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<username>
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>

```

터미널에서 명령을 실행할 때 백슬래시(\) 기호를 사용하여 특수 문자를 이스케이프하십시오.

- 8 셀을 다시 시작합니다.

```

service vmware-vcd restart

```

9 자동 스케일 권한 번들 게시

자동 스케일 권한 번들 게시

테넌트가 애플리케이션을 자동 스케일링하도록 하려면 시스템에 있는 하나 이상의 조직에 권한 번들을 게시해야 합니다. 자동 스케일링은 VMware Cloud Director 10.2.2부터 사용할 수 있습니다.

사전 요구 사항

자동 스케일 플러그인 구성 및 게시

절차

- 1 위쪽 탐색 모음에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **권한 번들**을 선택합니다.
- 3 자동 스케일링에 대한 액세스 권한을 부여하려는 테넌트 조직에 **레거시 권한 번들**이 없는지 확인합니다.
- 4 **vmware:scalegroup 사용 권한** 번들을 선택하고 **게시**를 클릭합니다.

5 번들을 게시하려면 다음을 수행합니다.

- a **테넌트에 게시**를 선택합니다.
- b 역할을 게시할 대상 조직을 선택합니다.
 - 시스템에 있는 기존 조직 및 새로 만든 조직 모두에 번들을 게시하려면 **모든 테넌트에 게시**를 선택합니다.
 - 시스템에 있는 특정 조직에 번들을 게시하려면 조직을 개별적으로 선택합니다.

6 **저장**을 클릭합니다.

다음에 수행할 작업

스케일 그룹을 사용하려는 테넌트 역할에 필요한 **VMWARE:SCALEGROUP** 권한을 추가합니다. 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"의 [글로벌 테넌트 역할 보기 및 편집](#)을 참조하십시오.

VMware Cloud Director 장치 데이터베이스 클러스터 상태 모니터링

VMware Cloud Director 장치 관리 사용자 인터페이스, 장치 API 또는 repmgr 오픈 소스 도구 제품군을 사용하여 VMware Cloud Director 장치 클러스터를 모니터링할 수 있습니다.

VMware Cloud Director 장치 관리 UI를 사용하여 장치 페일오버 모드를 볼 수도 있습니다. 페일오버 모드는 기본 데이터베이스가 실패할 경우 VMware Cloud Director를 통해 자동으로 데이터베이스 페일오버를 트리거할지 아니면 **시스템 관리자**가 수동으로 페일오버를 시작해야 하는지 나타냅니다.

노드 전체에서 페일오버 모드가 일관되지 않은 경우 페일오버 모드는 Indeterminate입니다.

Indeterminate 모드는 이전 기본 셀 이후 노드와 기타 노드 간에 일관성 없는 클러스터 상태를 초래할 수 있습니다. 문제를 진단하고 상황을 수동으로 해결해야 합니다.

VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기

VMware Cloud Director 장치 관리 사용자 인터페이스를 사용하여 클러스터 상태를 모니터링할 수 있습니다.

VMware Cloud Director 장치 관리 UI 또는 VMware Cloud Director 장치 API를 사용하여 클러스터의 셀의 이름, 셀의 역할, 셀 상태, 대기 셀이 따르는 셀의 이름, 클러스터 페일오버 모드를 볼 수 있습니다. 이 절차에서는 관리 UI에서 장치 클러스터 상태를 모니터링하는 단계를 설명합니다.

절차

1 https://primary_eth1_ip_address:5480에서 장치 관리 UI에 **루트**로 로그인합니다.

2 왼쪽 패널에서 **내장형 데이터베이스 가용성**을 선택합니다.

노드의 짧은 DNS 이름, 역할, 상태, 업스트림 노드(즉 현재 기본 노드)의 이름, 노드에서 사용 가능한 작업을 볼 수 있습니다.

다음 열에서 호스트 이름 앞의 물음표(?)는 현재 기본 노드에 연결할 수 없음을 나타냅니다. 호스트 이름 앞의 느낌표(!)는 현재 기본 노드의 메타데이터가 업데이트되지 않았으며 잘못되었을 수 있거나 노드가 현재 기본 노드에 연결되어 있지 않음을 나타냅니다. 이 문제는 장시간 다운타임 후 노드를 다시 시작하는 경우 발생할 수 있습니다. 노드를 기본 노드에 연결할 수 없는 경우에는 해당 노드를 등록 취소하고 새 대기 노드로 바꿔야 합니다.

3 클러스터 상태를 봅니다.

클러스터 상태	설명
정상	클러스터가 정상 상태입니다. 기본 셀과 두 대기 셀 모두 온라인 상태이고 작동이 가능합니다. VMware Cloud Director UI 및 API가 작동합니다.
성능 저하됨	클러스터가 성능 저하됨 상태입니다. 기본 셀과 대기 셀 중 하나가 온라인 상태이고 작동이 가능하지만 다른 대기 셀은 작동하지 않습니다. 이 상태에서는 기본 데이터베이스가 작동하지만 작동 가능한 셀 중 하나에 다른 데이터베이스 장애가 있는 경우 기본 데이터베이스가 작동하지 않게 됩니다. 클러스터를 Healthy 상태로 복원하려면 작동하지 않는 대기 셀을 가능한 한 빨리 작동하는 새 대기 셀로 교체해야 합니다. VMware Cloud Director UI 및 API가 작동합니다.
No_Active_Primary	작동 가능한 기본 데이터베이스가 없습니다. 작동 가능한 대기 셀이 두 개인 경우 둘 중 하나를 새 기본 셀로 승격시켜야 합니다. 환경에 두 개의 작동 가능한 대기 셀이 없는 경우 문제를 진단하고 상황을 수동으로 해결해야 합니다. VMware Cloud Director UI 및 API를 사용할 수 없습니다.
Read_Only_Primary	온라인 기본 데이터베이스가 있지만 환경에 작동 가능한 대기 셀이 없기 때문에 Read_Only입니다. 두 개의 새 대기 셀을 배포해야 합니다. VMware Cloud Director UI 및 API를 사용할 수 없습니다.
Critical_Problem	클러스터가 일관되지 않은 상태입니다. 예를 들어 둘 이상의 기본 셀이 온라인 상태이거나 대기 셀이 잘못된 기본 셀을 따릅니다. 문제를 진단하고 상황을 수동으로 해결해야 합니다. 이 상태는 VMware Cloud Director UI 및 API 가용성에 영향을 줄 수 있습니다.
SSH_Problem	SSH 문제는 postgres 사용자가 SSH를 통해 피어 데이터베이스 노드에 연결할 수 없음을 나타냅니다. 심각한 문제는 가능한 한 빨리 해결해야 합니다. 클러스터 상태가 SSH 문제를 나타냄의 내용을 참조하십시오. VMware Cloud Director UI 및 API가 완전히 작동되지 않을 수 있습니다.

4 장치 페일오버 모드를 봅니다.

페일오버 모드	설명
자동	기본 데이터베이스 장애가 발생하면 VMware Cloud Director가 자동으로 데이터베이스 페일오버를 트리거합니다.
수동	기본 데이터베이스 장애가 발생하면 VMware Cloud Director 장치 관리 UI 또는 페일오버 API를 사용하여 데이터베이스 페일오버를 시작해야 합니다.
미확정	클러스터의 모든 노드에서 페일오버 모드가 일관되지 않습니다. 문제를 진단하고 상황을 해결해야 합니다. VMware Cloud Director 장치 API를 사용하여 FailoverMode를 Manual 또는 Automatic으로 재설정합니다. "VMware Cloud Director 장치 API 스키마 참조" 에서 "페일오버 모드" 정보를 참조하십시오.

VMware Cloud Director 장치 서비스 상태 보기

VMware Cloud Director 장치 관리 사용자 인터페이스를 사용하여 VMware Cloud Director 장치 서비스의 상태를 모니터링할 수 있습니다.

[서비스] 탭에서 기본 및 대기 장치에 대한 vmware-vcd, vpostgres 및 appliance-sync.timer 서비스와 애플리케이션 셀에 대한 vmware-vcd 및 appliance-sync.timer 서비스를 모니터링할 수 있습니다.

appliance-sync.timer 서비스는 데이터베이스 HA 클러스터 또는 VMware Cloud Director 서버 그룹의 모든 노드 간에 관련 정보를 공유하는 appliance-sync.service를 정기적으로 실행합니다. appliance-sync.service는 장치 그룹에 있는 장치의 구성 파일을 읽고 쓰는 방법으로 VMware Cloud Director 장치 기능에 필요한 파일에 대한 정기적인 검사 및 동기화를 실행합니다. 타이머의 정상 상태는 waiting 및 running입니다.

절차

- 1 `https://primary_eth1_ip_address:5480`에서 장치 관리 UI에 **루트**로 로그인합니다.
- 2 왼쪽 패널에서 **서비스** 탭을 선택합니다.
- 3 VMware Cloud Director 서비스의 상태를 봅니다.

데이터베이스 고가용성 클러스터에서 연결 상태 확인

Replication Manager Tool Suite를 사용하여 데이터베이스 고가용성 클러스터의 노드 간 연결을 확인할 수 있습니다.

절차

- 1 클러스터에서 실행 중인 셀의 OS에 **root**로 로그인하거나 SSH를 통해 로그인합니다.

2 사용자를 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

3 클러스터의 연결을 확인합니다.

- `repmgr cluster matrix` 명령은 클러스터의 각 노드에서 `repmgr cluster show` 명령을 실행하고 결과를 매트릭스로 표시합니다.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/
repmgr.conf cluster matrix
```

다음 예에서는 노드 1과 노드 2가 작동 중이고 노드 3이 다운되었습니다. 각 행은 하나의 서버에 해당하며 이 서버에서 아웃바운드 연결을 테스트한 결과를 나타냅니다.

세 번째 행의 세 항목은 ? 기호로 표시됩니다. 노드 3이 다운되어 아웃바운드 연결에 대한 정보가 없기 때문입니다.

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	x
node 3	3	?	?	?

- `repmgr cluster crosscheck` 명령은 각 노드 조합 간 연결을 교차 확인하여 클러스터 연결에 대한 더 나은 개요를 제공할 수 있습니다.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/
repmgr.conf cluster crosscheck
```

다음 예에서 `repmgr cluster crosscheck` 명령을 실행하는 노드는 클러스터 매트릭스 시스템 출력을 다른 노드의 출력과 병합하고 노드 간의 교차 확인을 수행합니다. 이 예에서는 모든 노드가 작동하지만 노드 1에서 나와서 노드 3으로 향하는 패킷을 방화벽이 삭제합니다. 이것은 비대칭 네트워크 파티션의 예입니다. 여기서 노드 1은 노드 3으로 패킷을 전송할 수 없습니다.

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	*
node 3	3	*	*	*

다음에 수행할 작업

데이터베이스 고가용성 클러스터에서 전체 연결 상태를 확인하려면 각 노드에서 다음 명령을 실행하고 결과를 비교합니다.

데이터베이스 고가용성 클러스터에서 노드의 복제 상태 확인

Replication Manager Tool Suite 및 PostgreSQL 대화형 터미널을 사용하여 데이터베이스 고가용성 클러스터에서 개별 노드의 복제 상태를 확인할 수 있습니다.

절차

- 1 클러스터에서 실행 중인 노드의 OS에 **root**로 로그인하거나 SSH를 통해 로그인합니다.
- 2 사용자를 **postgres**로 변경합니다.

```
sudo -i -u postgres
```

- 3 노드의 복제 상태를 확인합니다.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf  
node status
```

기본 노드에 대한 시스템 출력은 노드 정보, PostgreSQL 버전에 대한 정보 및 복제 세부 정보를 제공합니다. 예는 다음과 같습니다.

```
Node "bos1-vcloud-static-161-5":  
  PostgreSQL version: 10.9  
  Total data size: 81 MB  
  Conninfo: host=172.18.36.193 user=repmgr dbname=repmgr connect_timeout=2  
  Role: primary  
  WAL archiving: off  
  Archive command: (none)  
  Replication connections: 2 (of maximal 10)  
  Replication slots: 0 physical (of maximal 10; 0 missing)  
  Replication lag: n/a
```

대기 노드에 대한 시스템 출력은 노드 정보, PostgreSQL 버전에 대한 정보, 복제 세부 정보 및 업스트림 노드에 대한 정보를 제공합니다. 예는 다음과 같습니다.

```
Node "bos1-vcloud-static-161-49":  
  PostgreSQL version: 10.9  
  Total data size: 83 MB  
  Conninfo: host=172.18.36.191 user=repmgr dbname=repmgr connect_timeout=2  
  Role: standby  
  WAL archiving: off  
  Archive command: (none)  
  Replication connections: 0 (of maximal 10)  
  Replication slots: 0 physical (of maximal 10; 0 missing)  
  Upstream node: bos1-vcloud-static-161-48 (ID: 683)  
  Replication lag: 0 seconds  
  Last received LSN: 2/D863B4E0  
  Last replayed LSN: 2/D863B4E0
```

- 4 (선택 사항) 자세한 정보를 보려면 PostgreSQL 대화형 터미널을 사용하여 노드의 복제 상태를 확인하십시오.

PostgreSQL 대화형 터미널은 대기 노드의 수신된 로그 레코드가 기본 노드가 보낸 로그보다 뒤쳐져 있는지 여부에 대한 정보를 제공할 수 있습니다.

- a psql 터미널에 연결합니다.

```
/opt/vmware/vpostgres/current/bin/psql
```

- b 디스플레이를 확장하고 쿼리 결과를 읽기 쉽게 만들려면 `set \x` 명령을 실행합니다.
- c 노드의 역할에 따라 복제 상태 쿼리를 실행합니다.

옵션	작업
기본 노드에서 쿼리를 실행합니다.	<code>select* from pg_stat_replication;</code>
대기 노드에서 쿼리를 실행합니다.	<code>select* from pg_stat_wal_receiver;</code>

VMware Cloud Director 서비스 상태 확인

VMware Cloud Director 장치의 관리 UI를 사용하여 로그인한 셀에 대한 VMware Cloud Director 서비스의 상태를 볼 수 있습니다.

절차

- 1 `https://primary_eth1_ip_address:5480`에서 장치 관리 UI에 **루트**로 로그인합니다.
- 2 서비스의 상태를 보려면 왼쪽 패널에서 **서비스**를 선택합니다.

VMware Cloud Director 장치가 제대로 작동 중이라면 `vmware-vcd` 및 `vpostgres` 서비스가 실행되고 있어야 합니다.

다음에 수행할 작업

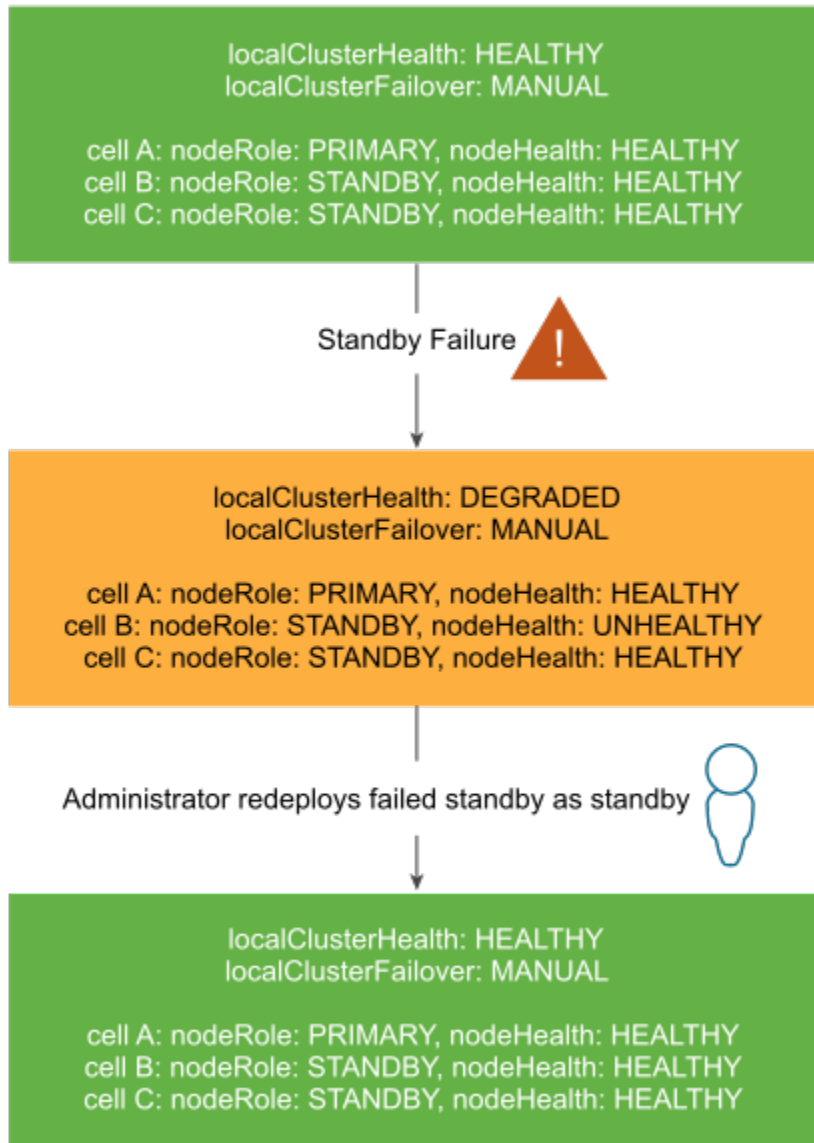
디버깅 목적으로 `repmgrd` 서비스의 상태를 확인해야 하는 경우에는 VMware Cloud Director 장치 API를 사용해야 합니다.

VMware Cloud Director 장치 데이터베이스 클러스터 복구

데이터베이스 또는 VMware Cloud Director 노드 중 하나에 장애가 있는 경우 데이터베이스 클러스터를 복구할 수 있습니다.

데이터베이스 고가용성 클러스터의 셀이 실패할 경우, 어떤 실패가 발생했고 어떻게 문제를 해결할 수 있는지가 클러스터 상태에 표시됩니다. 예를 들어 Degraded 클러스터 상태는 대기 셀과 관련된 실패를 나타냅니다. 시스템 관리자는 실패한 셀을 다시 배포해야 합니다.

그림 3-4. 대기 셀 실패에서 복구



데이터베이스 고가용성 클러스터의 기본 셀이 실패하면 클러스터 상태가 No_Active_Primary로 변경될 수 있습니다. 이는 시스템 관리자가 실패한 기본 셀을 복구해야 함을 나타냅니다.

고가용성 클러스터에서 기본 셀 장애로부터 복구

기본 셀이 제대로 실행되고 있지 않은 경우 VMware Cloud Director 데이터베이스를 복구하려면 대기 셀 중 하나가 새 기본 셀이 되어야 하며 새 대기를 배포해야 합니다. 장애 모드에 따라 VMware Cloud Director 장치가 자동으로 대기 셀을 새 기본으로 승격하거나 사용자가 수동으로 승격해야 합니다.

VMware Cloud Director 장치의 페일오버 모드에 따라 기본 셀 장애로부터 복구하는 두 가지 다른 워크플로가 있습니다. 이러한 워크플로를 사용하여 새 대기 셀을 배포할 때 실패한 기본 셀의 IP 주소와 호스트 이름을 재사용할 수 있습니다.

수동 페일오버 모드에 대한 복구 워크플로

기본 셀이 Not reachable 또는 Failed 상태이고 2개의 대기 셀이 Running 상태인 경우 장치 HTML5 사용자 인터페이스 및 VMware Cloud Director 장치 API를 사용하여 장애로부터 복구할 수 있습니다.

클러스터의 셀 상태를 보려면 [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.

- 1 가능한 경우 셀 관리 도구를 사용하여 VMware Cloud Director 프로세스를 종료합니다. 실패한 기본 셀에서 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <sysadmin user> cell --shutdown
```

- 2 실패한 기본 VM의 전원을 끕니다.
 - 3 대기 셀이 새 기본 항목이 되도록 승격합니다.
 - a 실행 중인 대기 셀의 장치 관리 UI(https://standby_ip_address:5480)에 **root**로 로그인합니다.
 - b 새 기본 셀로 사용할 대기 셀의 **역할** 열에서 **승격**을 클릭합니다.

관리 UI에 기본 역할이 있는 두 개의 셀이 표시됩니다. 원래 기본 항목은 실패 상태이고 새 기본 항목은 실행 중 상태입니다. 클러스터 상태는 성능 저하됩니다.
 - 4 실패한 기본 이외의 셀에서 장치 API Unregister 메서드를 사용하여 실패한 기본 장치를 repmgr 고가용성 클러스터에서 제거합니다. [VMware Cloud Director 장치 API](#) 설명서를 참조하십시오.
 - 5 실패한 기본 장치를 VMware Cloud Director 서버 그룹에서 제거합니다.
 - a Service Provider Admin Portal에 **관리자**로 로그인합니다.
 - b 위쪽 탐색 모음의 **리소스**에서 **클라우드 리소스**를 선택합니다.
 - c 왼쪽 창에서 **클라우드 셀**을 클릭합니다.
 - d 비활성 셀을 선택하고 **등록 취소**를 클릭합니다.
 - 6 실패한 기본 장치의 IP 주소와 호스트 이름을 재사용하려면 실패한 기본 장치의 전원이 꺼진 상태로 유지되도록 하거나 vSphere Client를 사용하여 삭제합니다.
 - 7 새로운 대기 장치를 배포합니다. [VMware Cloud Director 장치 배포](#) 시작하거나 [VMware OVF Tool을 사용하여 VMware Cloud Director 장치 배포](#)할 수 있습니다.
- 새 대기를 배포한 후에는 클러스터 상태가 정상이어야 합니다.
- 8 복원 전에 VMware Cloud Director 장치 FIPS 모드가 켜져 있는 경우 VMware Cloud Director 장치 API를 사용하여 다시 설정해야 합니다.
- 셀 FIPS 모드는 자동으로 복원됩니다.

자동 페일오버 모드 복구

기본 항목이 Failed 상태인 경우에는 VMware Cloud Director가 대기 셀을 새로운 실행 기본 항목으로 자동 승격합니다. 다만, 실행 중인 대기 셀이 하나만 있기 때문에 클러스터가 성능 저하된 상태입니다.

HTML5 사용자 인터페이스 및 VMware Cloud Director 장치 API를 사용하여 장애로부터 복구할 수 있습니다.

클러스터의 셀 상태를 보려면 [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.

- 1 가능한 경우 셀 관리 도구를 사용하여 VMware Cloud Director 프로세스를 종료합니다. 실패한 기본 셀에서 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <sysadmin user> cell --shutdown
```

- 2 실패한 기본 VM의 전원을 끕니다.

관리 UI에 기본 역할이 있는 두 개의 셀이 표시됩니다. 원래 기본 항목은 실패 상태이고 새 기본 항목은 실행 중 상태입니다. 클러스터 상태는 성능 저하된 상태입니다.

- 3 실패한 기본 이외의 셀에서 장치 API Unregister 메서드를 사용하여 실패한 기본 장치를 repmgr 고 가용성 클러스터에서 제거합니다. [VMware Cloud Director 장치 API](#) 설명서를 참조하십시오.
- 4 실패한 기본 장치를 VMware Cloud Director 서버 그룹에서 제거합니다.
 - a Service Provider Admin Portal에 **관리자**로 로그인합니다.
 - b 위쪽 탐색 모음의 **리소스**에서 **클라우드 리소스**를 선택합니다.
 - c 왼쪽 창에서 **클라우드 셀**을 클릭합니다.
 - d 비활성 셀을 선택하고 **등록 취소**를 클릭합니다.
- 5 실패한 기본 장치의 IP 주소와 호스트 이름을 재사용하려면 실패한 기본 장치의 전원이 꺼진 상태로 유지되도록 하거나 vSphere Client를 사용하여 삭제합니다.
- 6 새로운 대기 장치를 배포합니다. [VMware Cloud Director 장치 배포 시작](#)하거나 [VMware OVF Tool](#)을 사용하여 [VMware Cloud Director 장치 배포](#)할 수 있습니다. 새 대기를 배포한 후에는 클러스터 상태가 정상이어야 합니다.
- 7 실패한 기본 셀 이외의 다른 셀에서 장치 API Failover 메서드를 사용하여 클러스터 페일오버 모드를 Automatic으로 재설정합니다. [VMware Cloud Director 장치 API](#) 설명서를 참조하십시오.
- 8 복원 전에 VMware Cloud Director 장치 FIPS 모드가 켜져 있는 경우 VMware Cloud Director 장치 API를 사용하여 다시 설정해야 합니다.
셀 FIPS 모드는 자동으로 복원됩니다.

고가용성 클러스터에서 대기 셀 장애로부터 복구

대기 셀이 제대로 실행되고 있지 않은 경우 새 대기 셀을 배포하여 장애로부터 복구할 수 있습니다.

대기 셀 중 하나가 Not reachable 또는 Failed 상태인 경우 새 셀을 배포할 수 있습니다. 클러스터의 셀 상태를 보려면 [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.

이 워크플로를 사용하여 새 대기 셀을 배포할 때 실패한 대기 셀의 IP 주소와 호스트 이름을 재사용할 수 있습니다.

- 1 가능한 경우 셀 관리 도구를 사용하여 VMware Cloud Director 프로세스를 종료합니다. 실패한 대기 셀에서 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

- 2 실패한 대기 VM의 전원을 끕니다.
- 3 실패한 대기 셀 이외의 셀에서 장치 API Unregister 메서드를 사용하여 실패한 대기 셀을 repmgr 고가용성 클러스터에서 제거합니다. [VMware Cloud Director 장치 API](#) 설명서를 참조하십시오.
- 4 Service Provider Admin Portal을 사용하여 VMware Cloud Director 서버 그룹에서 실패한 대기 장치를 제거합니다.
 - a 위쪽 탐색 모음의 리소스에서 클라우드 리소스를 선택합니다.
 - b 왼쪽 창에서 클라우드 셀을 클릭합니다.
 - c 비활성 셀을 선택하고 등록 취소를 클릭합니다.
- 5 실패한 대기 셀의 IP 주소와 DNS 이름을 재사용하려면 실패한 대기 셀의 전원이 꺼진 상태로 유지되도록 하거나 삭제해야 합니다.
- 6 새로운 대기 장치를 배포합니다. [VMware Cloud Director 장치 배포](#) 시작하거나 [VMware OVF Tool](#)을 사용하여 [VMware Cloud Director 장치 배포](#)할 수 있습니다.
새 대기를 배포한 후에는 클러스터 상태가 정상이어야 합니다.
- 7 클러스터 페일오버 모드를 Automatic으로 재설정하려면, 실패한 대기 셀 이외의 셀에서 장치 API Failover 메서드를 사용합니다. [VMware Cloud Director 장치 API](#) 설명서를 참조하십시오.
자동 페일오버 모드에 대한 자세한 내용은 [VMware Cloud Director 장치의 자동 페일오버 항목](#)을 참조하십시오.
- 8 복원 전에 VMware Cloud Director 장치 FIPS 모드가 켜져 있는 경우 VMware Cloud Director 장치 API를 사용하여 다시 설정해야 합니다.
셀 FIPS 모드는 자동으로 복원됩니다.

데이터베이스 고가용성 클러스터에서 실패한 기본 또는 대기 셀 등록 취소

데이터베이스 고가용성 클러스터의 기본 또는 대기 노드가 실패하는 경우 VMware Cloud Director API를 사용하여 실패한 노드의 등록을 취소하고 클러스터에서 제거하여 일관성 없는 클러스터 상태 데이터를 방지할 수 있습니다.

VMware Cloud Director API 사용에 대한 자세한 내용은 <https://developer.vmware.com/>의 VMware Cloud Director 장치 API 설명서에서 UNREGISTER API 메서드를 참조하십시오.

사전 요구 사항

- 등록을 취소할 노드가 비활성 상태인지 확인하고 이름을 기록해 둡니다. 셀의 상태 및 대기 셀이 따르는 셀의 이름에 대한 자세한 내용은 [VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기](#)의 내용을 참조하십시오.
- 기본 노드의 등록을 취소하려면 실패한 기본 노드가 비활성이고 다음 대기 노드가 없는지 확인하고 새 기본 노드를 승격합니다.

절차

- ◆ 비활성 노드를 제거하려면 명령을 실행할 활성 노드에 대해 DELETE 요청을 수행합니다.

```
DELETE https://<Active_Node_FQDN>:5480/api/1.0.0/nodes/<Inactive_Node_Name>
```

장치 문제 해결

VMware Cloud Director 장치 배포가 실패하거나 장치가 제대로 작동하지 않으면, 장치 로그 파일을 검토하여 문제의 원인을 파악할 수 있습니다.

VMware 기술 지원은 주기적으로 진단 정보 처리 지원을 요청합니다. vmware-vcd-support 스크립트를 사용하여 호스트 로그 정보와 VMware Cloud Director 로그를 수집할 수 있습니다. VMware Cloud Director의 진단 정보 수집에 대한 자세한 내용은 <https://kb.vmware.com/s/article/1026312> 항목을 참조하십시오. vmware-vcd-support 스크립트를 실행하면, 사용 중지되거나 교체된 셀에 대한 정보가 실패 상태로 로그에 포함될 수 있습니다. <https://kb.vmware.com/s/article/71349>의 내용을 참조하십시오.

VMware Cloud Director 장치의 로그 파일 검토

VMware Cloud Director 장치를 배포한 후에 firstboot 및 데이터베이스 로그에서 오류 및 경고를 검토할 수 있습니다.

절차

- 1 VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 /opt/vmware/var/log로 이동합니다.
- 3 로그 파일을 검토합니다.
 - firstboot 파일에는 장치의 첫 번째 부팅과 관련된 로깅 정보가 포함되어 있습니다.
 - /opt/vmware/var/log/vcd/ 디렉토리에는 Replication Manager(repmgr) 도구 집합 설정과 재구성 및 장치 동기화와 관련된 로그가 포함되어 있습니다.
 - /opt/vmware/var/log/vcd/pg/ 디렉토리에는 내장형 장치 데이터베이스의 백업과 관련된 로그가 포함되어 있습니다.

- /opt/vmware/etc/vami/ovfEnv.xml 파일에는 배포 OVF 매개 변수가 포함되어 있습니다.

장치 배포 후 VMware Cloud Director 셸이 시작되지 않음

VMware Cloud Director 장치를 성공적으로 배포했지만 VMware Cloud Director 서비스가 시작되지 않을 수 있습니다.

문제

장치 배포 후 vmware-vcd 서비스가 비활성 상태입니다.

원인

기본 셸을 배포한 경우 미리 채워진 NFS 공유 전송 서비스 스토리지로 인해 VMware Cloud Director 서비스가 시작되지 않을 수 있습니다. 기본 장치를 배포하기 전에 공유 전송 서비스 스토리지에 responses.properties 파일이나 appliance-nodes 디렉토리가 포함되어지 않아야 합니다.

대기 셸이나 vCD 애플리케이션 셸을 배포한 경우에는 NFS 공유 전송 스토리지에 responses.properties 파일이 누락되어 VMware Cloud Director 서비스가 시작되지 않을 수 있습니다. 대기 또는 vCD 애플리케이션 장치를 배포하기 전에 공유 전송 서비스 스토리지에 responses.properties 파일이 포함되어 있어야 합니다.

참고 클러스터가 자동 페일오버에 대해 구성되어 있다면 하나 이상의 추가 셸을 배포한 후 장치 API를 사용하여 클러스터 페일오버 모드를 Automatic으로 재설정해야 합니다. **VMware Cloud Director 장치 API**를 참조하십시오. 새 셸에 대한 기본 페일오버 모드는 Manual입니다. 클러스터의 노드 전체에서 페일오버 모드가 일관되지 않은 경우 클러스터 페일오버 모드는 Indeterminate입니다. Indeterminate 모드는 이전 기본 셸 이후 노드와 기타 노드 간에 일관성 없는 클러스터 상태를 초래할 수 있습니다. 클러스터 페일오버 모드를 보려면 **VMware Cloud Director 장치 클러스터 상태 및 페일오버 모드 보기**의 내용을 참조하십시오.

해결책

- 1 VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 /opt/vmware/var/log/vcd/setupvcd.log에서 NFS 스토리지와 관련된 오류 메시지를 검토합니다.
- 3 장치 유형에 대한 NFS 스토리지를 준비합니다.
- 4 셸을 다시 배포합니다.

초기 장치 구성 중에 NFS 검증 후 복구에 실패함

초기 VMware Cloud Director 장치 구성 중에 공유 스토리지 검증이 실패하는 경우 배포자가 문제를 해결하는 데 사용할 수 있는 오류 메시지를 표시합니다.

문제

VMware Cloud Director 장치 배포 중 배포자가 NFS 공유를 참조하는 오류 메시지를 표시합니다.

원인

VMware Cloud Director에 대한 전송 서버 스토리지를 준비하지 않으면 배포 중 NFS 검증이 실패합니다.

해결책

버전	오류	작업
10.2	UID가 999인 알 수 없는 사용자가 /opt/vmware/vcloud-director/data/transfer/xyz를 소유하고 있습니다. 1003이 필요합니다.	NFS 서버에서 vcloud 사용자의 사용자 ID 구성을 확인합니다. vcloud 사용자 ID는 NFS 서버 및 장치에서 동일한 값을 가져야 합니다.
10.2	GID가 999인 알 수 없는 사용자가 /opt/vmware/vcloud-director/data/transfer/xyz를 소유하고 있습니다. 1002가 필요합니다.	NFS 서버에서 vcloud 사용자의 그룹 ID 구성을 확인합니다. vcloud 사용자 ID는 NFS 서버 및 장치에서 동일한 값을 가져야 합니다.
10.2	전송 공유에서 파일을 변경할 수 없습니다.	장치가 마운트된 NFS 공유에 쓸 수 없는 이유를 확인합니다. 쓸 수 없는 이유를 확인하려면 다른 Linux 시스템을 사용하여 NFS 공유를 다시 마운트해 봅니다.
10.2	/usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test 중에 시간 초과가 발생했습니다. 기간: 5초	이 장치가 5초 내에 지정된 NFS 공유를 마운트할 수 없는 이유를 확인합니다. NFS 공유를 적시에 마운트할 수 없는지 확인하려면 다른 Linux 시스템을 사용하여 마운트해 봅니다. 또는 이 NFS 공유에 대한 NFS 서버 내보내기 설정을 확인합니다.
10.2	/usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test 중에 오류가 발생했습니다.	이 장치가 지정된 NFS 공유를 마운트할 수 없는 이유를 확인합니다. NFS 공유를 마운트할 수 없는지 확인하려면 다른 Linux 시스템을 사용하여 마운트해 봅니다. 또는 이 NFS 공유에 대한 NFS 서버 내보내기 설정을 확인합니다.
10.2	전송 공유 디렉토리 /opt/vmware/vcloud-director/data/transfer가 없습니다.	전송 공유 디렉토리 또는 마운트 지점이 없습니다. 해당 디렉토리를 생성합니다.
10.2	touch xyz 작업을 수행하는 동안 /opt/vmware/vcloud-director/data/transfer/xyz 파일에 예기치 않은 사용 권한이 있습니다. 필요한 권한: root root 644. 찾은 권한: root, root, 600	NFS 전송 공유에서 지정된 작업을 수행한 후에 파일 소유자, 그룹 또는 사용 권한이 예상 값에서 지연되는 이유를 확인하고 문제를 해결합니다.

버전	오류	작업
10.2	NFS 서버 클럭이 장치 클럭에 대해 동기화되지 않았습니다. 시간 차이: 3 분, 12초	NFS 서버 및 장치의 시간 설정을 확인합니다. 둘 중 하나 또는 둘 다 정확하지 않은 경우 올바른 시간으로 설정하고 NTP를 사용하여 동기화되었는지 확인합니다.
10.2	chmod xyz 작업을 수행하는 동안 /opt/vmware/vcloud-director/data/transfer/xyz 파일에 예기치 않은 사용 권한이 있습니다. 필요한 권한: root root 750. 찾은 권한: root, root, 700	NFS 전송 공유에서 지정된 작업을 수행한 후에 파일 소유자, 그룹 또는 사용 권한이 예상 값에서 지연되는 이유를 확인하고 문제를 해결합니다.
10.2	chown xyz 작업을 수행하는 동안 /opt/vmware/vcloud-director/data/transfer/xyz 파일에 예기치 않은 사용 권한이 있습니다. 필요한 권한: root root 750. 찾은 권한: root, root, 700	NFS 전송 공유에서 지정된 작업을 수행한 후에 파일 소유자, 그룹 또는 사용 권한이 예상 값에서 지연되는 이유를 확인하고 문제를 해결합니다.
10.2 이상	명령 인수가 잘못되었거나 누락되었습니다. 사용: nfsValidate <i>nfs_mount_string</i>	JSON 요청 본문을 구문 분석할 수 없습니다. 올바른 JSON 요청 본문을 제공합니다.
10.2 이상	빈 nfs_mount 문자열	NFS 마운트 문자열이 요청 본문에 없습니다. NFS 마운트 문자열 인수를 제공합니다.
10.2 이상	잘못된 nfs_mount 문자열: <i>nfs_mount_string_argument</i>	NFS 마운트 문자열을 올바른 형식으로 변경합니다. <i>IP_address:path</i>
10.2 이상	잘못된 셀 유형: <i>cell_type_string</i>	셀 유형은 primary, standby 또는 cell 이어야 합니다. OVF 매개 변수가 이러한 값과 같지 않으면 장치 구성을 확인합니다.
10.2 이상	필수 OS 구성이 완료되지 않았습니다	/opt/vmware/appliance/etc/os-configuration-completed 파일이 장치에 없습니다. 운영 체제를 구성합니다.
10.2 이상	Cloud Director 장치 시스템 설정이 이미 완료되었습니다.	장치에서 /opt/vmware/appliance/etc/vcd-configuration-completed 파일을 찾았습니다. 클라우드 디렉토리 설정이 이미 완료되었으므로 이 스크립트를 실행하면 안 됩니다.
10.2 이상	10.150.170.3:/data/transfer/cells 디렉토리가 이미 있습니다. 기본 장치를 사용하려면 이를 제거해야 합니다.	기본 장치에 이 디렉토리가 있어서는 안 됩니다. NFS 서버에 이 디렉토리가 있으므로 제거해야 합니다.

버전	오류	작업
10.2 이상	10.150.170.3:/data/transfer/appliance-nodes 디렉토리가 이미 있습니다. 기본 장치를 사용하려면 이를 제거해야 합니다.	기본 장치에 이 디렉토리가 있어서는 안 됩니다. NFS 서버에 이 디렉토리가 있으므로 제거해야 합니다.
10.2 이상	responses.properties 파일이 전송 공유에 이미 있습니다. 기본 장치를 사용하려면 이를 제거해야 합니다.	기본 장치에 responses.properties 파일이 있어서는 안 됩니다. 제거해야 합니다.
10.2 이상	responses.properties 파일이 전송 공유에 없습니다. 대기 또는 셀 장치에 이 파일이 있어야 합니다.	대기 또는 셀 장치에 responses.properties 파일이 있어야 합니다. 기본 장치가 아직 구성되지 않았을 수 있습니다. 추가 셀을 구성하기 전에 기본 장치를 구성해야 합니다.
10.2 이상	시스템 설정이 진행 중인 동안에는 nfsValidate를 실행할 수 없습니다.	nfsValidate 실행을 시도하기 전에 시스템 설정이 완료될 때까지 기다립니다.
10.2 이상	/opt/vmware/vcloud-director/data/nfs-test 스크립트에서 사용할 tmp 디렉토리를 만들 수 없습니다.	파일 시스템 사용 권한을 확인하여 이 디렉토리를 만들 수 없는 이유를 확인합니다.
10.2.1	제공된 NFS 공유에 파일을 생성할 수 없습니다. 쓰기가 불가능할 수 있습니다. 내보낸 NFS 파일 시스템이 읽기 전용이거나 no_root_squash가 지정되지 않았기 때문일 수 있습니다.	장치가 마운트된 NFS 공유에 쓸 수 없는 이유를 확인합니다. 쓸 수 없는 이유를 확인하려면 다른 Linux 시스템을 사용하여 NFS 공유를 다시 마운트해 봅니다.
10.2.1	제공된 전송 공유에서 파일에 chmod를 실행할 수 없습니다.	장치가 마운트된 NFS 공유에서 파일 시스템 개체에 대한 액세스 권한을 변경할 수 없는 이유를 확인합니다. 다른 Linux 시스템을 사용하여 NFS 공유를 마운트해 봅니다.
10.2.1	제공된 전송 공유에서 파일에 chown을 실행할 수 없습니다.	장치가 마운트된 NFS 공유에서 파일 시스템 개체의 소유자를 변경할 수 없는 이유를 확인합니다. 다른 Linux 시스템을 사용하여 NFS 공유를 마운트해 봅니다.
10.2.1	마운트 중 시간 초과 발생	이 장치가 5초 내에 지정된 NFS 공유를 마운트할 수 없는 이유를 확인합니다. NFS 공유를 적시에 마운트할 수 없는지 확인하려면 다른 Linux 시스템을 사용하여 마운트해 봅니다. 또는 이 NFS 공유에 대한 NFS 서버 내보내기 설정을 확인합니다.
10.2.1	마운트 중 오류 발생	이 장치가 지정된 NFS 공유를 마운트할 수 없는 이유를 확인합니다. NFS 공유를 마운트할 수 없는지 확인하려면 다른 Linux 시스템을 사용하여 마운트해 봅니다. 또는 이 NFS 공유에 대한 NFS 서버 내보내기 설정을 확인합니다.

버전	오류	작업
10.2.1	제공된 NFS 공유를 UID가 123인 알 수 없는 사용자가 소유합니다. 필요한 권한: root제공된 NFS 공유를 GID가 456인 알 수 없는 그룹이 소유합니다. 필요한 권한: root	NFS 전송 공유에서 지정된 작업을 수행한 후 예상된 파일 소유자, 그룹 또는 양쪽 모두가 예상된 값에서 지연되는 이유를 확인하고 문제를 해결합니다.
10.2.1	제공된 NFS 공유에 대해 예상하지 못한 소유권 및/또는 사용 권한입니다. 필요한 권한: root:root , 모드: 750. 찾은 권한: root:root, 모드: 777	NFS 전송 공유에서 지정된 작업을 수행한 후 파일 소유자, 그룹 및 모드에 대한 예상 값 중 일부 또는 전부가 예상과 다른 이유를 확인합니다. 문제를 해결합니다.
10.2.1	NFS 서버 클럭이 장치 클럭에 대해 동기화되지 않았습니다. 시간 차이: 1:55:14.603510	NFS 서버 및 장치의 시간 설정을 확인합니다. 둘 중 하나 또는 둘 다 정확하지 않은 경우 올바른 시간으로 설정하고 NTP를 사용하여 동기화되었는지 확인합니다.

VMware Cloud Director 장치에 마이그레이션하거나 복원할 때 VMware Cloud Director 서비스를 재구성하지 못함

VMware Cloud Director 장치에 마이그레이션하거나 복원할 때 `configure` 명령을 실행하면 실패할 수 있습니다.

문제

VMware Cloud Director를 새 VMware Cloud Director 장치 환경으로 마이그레이션하거나 복원하는 절차 중에 각각 0,; 새 셀에서 `configure` 명령을 실행하여 VMware Cloud Director 서비스를 재구성합니다. `configure` 명령이 실패하고 다음 오류 메시지가 표시될 수 있습니다.

```
sun.security.validator.ValidatorException: PKIX 경로 유효성 검사 실패:
java.security.cert.CertPathValidatorException: 서명 확인 실패.
```

해결책

- 1 대상 셀에서 다음 명령을 실행합니다.

```
sed -i 'vcd_ova.crt/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh
```

- 2 1분 동안 기다린 후 `configure` 명령을 다시 실행합니다.

VMware Cloud Director 장치 대기 노드에 연결할 수 없는 상태가 됨

VMware Cloud Director는 노드 간의 동기식 스트리밍 복제를 유지 관리합니다. 대기 노드에 연결할 수 없는 상태가 되면 원인을 파악하고 문제를 해결해야 합니다.

문제

VMware Cloud Director 장치 관리 UI에 클러스터 상태가 DEGRADED으로 표시되고 대기 노드 중 하나의 상태가 연결할 수 없음입니다.

/nodes API는 localClusterHealth가 DEGRADED이고 노드 status는 연결할 수 없음이며 nodeHealth가 UNHEALTHY이라는 정보를 반환합니다.

예를 들어 /nodes API가 노드에 대해 다음 정보를 반환할 수 있습니다.

```
{
  "localClusterFailover": "MANUAL",
  "localClusterHealth": "DEGRADED",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": primary_node_ID,
      "location": "default",
      "name": "primary_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "PRIMARY",
      "role": "primary",
      "status": "* running",
      "upstream": ""
    },
    {
      "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover state unknown - unable to ssh to failed or unreachable
node",
        "mode": "UNKNOWN",
        "repmgrd": {
          "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = n/a",
          "status": "UNKNOWN"
        }
      },
      "id": unreachable_standby_node_ID,
      "location": "default",
      "name": "unreachable_standby_host_name",
      "nodeHealth": "UNHEALTHY",
      "nodeRole": "STANDBY",
      "role": "standby",
      "status": "? unreachable",
      "upstream": "primary_host_name"
    },
    {
      "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
```

```

connect_timeout=2",
    "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
            "details": "On node running_standby_node_ID (running_standby_host_IP):
repmgrd = not applicable",
            "status": "NOT APPLICABLE"
        }
    },
    "id": running_standby_node_ID,
    "location": "default",
    "name": "running_standby_host_name",
    "nodeHealth": "HEALTHY",
    "nodeRole": "STANDBY",
    "role": "standby",
    "status": "running",
    "upstream": "primary_host_name"
}
],
"warnings": [
    "unable to connect to node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID)",
    "node \"unreachable_standby_host_name\" (ID: unreachable_standby_node_ID) is
registered as an active standby but is unreachable"
]
}

```

원인

데이터 무결성을 보장하기 위해 PostgreSQL 데이터베이스는 WAL(Write-Ahead Logging)을 사용합니다. 기본 노드는 복제 및 복구 목적으로 WAL을 활성 대기 노드로 지속적으로 스트리밍합니다. 대기 노드는 WAL을 수신할 때 처리합니다. 대기 노드에 연결할 수 없는 경우 WAL 수신을 중지하며, 새로운 기본 노드로 승격할 후보가 될 수 없습니다.

해결책

- ◆ 연결할 수 없는 대기 노드의 가상 시스템이 실행되고 있는지 확인합니다.
- ◆ 대기 노드에 대한 네트워크 연결이 작동하는지 확인합니다.
- ◆ 대기 노드가 다른 노드와 통신하지 못하게 할 수 있는 SSH 문제가 없는지 확인합니다.
- ◆ 대기 노드의 vpostgres 서비스가 실행 중인지 확인합니다.

다음에 수행할 작업

네트워크 또는 SSH 문제가 없는지 확인하려면 데이터베이스 고가용성 클러스터에서 [연결 상태 확인](#) 항목을 참조하십시오.

VMware Cloud Director 장치 대기 노드가 연결되지 않은 상태가 됨

VMware Cloud Director는 노드 간의 동기식 스트리밍 복제를 유지 관리합니다. 대기 노드가 연결되지 않은 상태가 되면 원인을 파악하고 문제를 해결해야 합니다.

문제

VMware Cloud Director 장치 관리 UI에 클러스터 상태가 DEGRADED으로 표시되고, 연결되지 않은 대기 노드 중 하나의 상태가 실행 중이며 대기 노드의 업스트림 노드 이름 앞에 느낌표(!)가 있습니다.

PostgreSQL 로그에는 기본 노드가 WAL 세그먼트를 삭제한 것으로 표시됩니다.

```
2020-10-08 04:10:50.064 UTC [13390] LOG:  started streaming WAL from primary at 21/800000000
on timeline 17
2020-10-08 04:10:50.064 UTC [13390] FATAL:  could not receive data from WAL stream: ERROR:
requested WAL segment 00000011000000021000000080 has already been removed
2020-10-08 04:10:55.047 UTC [13432] LOG:  started streaming WAL from primary at 21/800000000
on timeline 17
2020-10-08 04:10:55.047 UTC [13432] FATAL:  could not receive data from WAL stream: ERROR:
requested WAL segment 00000011000000021000000080 has already been removed
```

/nodes API는 localClusterHealth가 DEGRADED, 노드 status가 실행 중, nodeHealth가 HEALTHY이라는 정보를 반환합니다. 대기 노드의 업스트림 노드 이름 앞에 느낌표(!)가 있고 /nodes API는 대기 노드가 업스트림 노드에 연결되지 않았다는 경고를 반환합니다.

예를 들어 /nodes API가 노드에 대해 다음 정보를 반환할 수 있습니다.

```
{
  "localClusterFailover": "MANUAL",
  "localClusterHealth": "DEGRADED",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
          "status": "NOT APPLICABLE"
        }
      },
      "id": primary_node_ID,
      "location": "default",
      "name": "primary_host_name",
      "nodeHealth": "HEALTHY",
      "nodeRole": "PRIMARY",
      "role": "primary",
      "status": "* running",
      "upstream": ""
    },
    {
```

```

        "connectionString": "host=unattached_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node unattached_standby_node_ID
(unattached_standby_host_name): repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": unattached_standby_node_ID,
        "location": "default",
        "name": "unattached_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "! upstream_host_name"
    },
    {
        "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": running_standby_node_ID,
        "location": "default",
        "name": "running_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "upstream_host_name"
    }
],
"warnings": [
    "node \"unattached_standby_host_name\" (ID: unattached_standby_node_ID) is not
attached to its upstream node \"upstream_host_name\" (ID: upstream_node_id)"
]
}

```

대기 노드가 연결되지 않은 상태가 되면 가능한 한 빨리 다시 연결해야 합니다. 노드가 너무 오랫동안 연결되지 않은 상태로 유지되면 기본 노드에서 복제를 재개하는 것이 불가능할 만큼 지속적으로 스트리밍되는 WAL 레코드를 처리하는 것이 뒤쳐질 수 있습니다.

원인

데이터 무결성을 보장하기 위해 PostgreSQL 데이터베이스는 WAL(Write-Ahead Logging)을 사용합니다. 기본 노드는 복제 및 복구 목적으로 WAL을 활성 대기 노드로 지속적으로 스트리밍합니다. 대기 노드는 WAL을 수신할 때 처리합니다. 대기 노드가 연결되지 않은 상태가 되면 WAL 수신을 중지하며, 새로운 기본 노드로 승격할 후보가 될 수 없습니다.

해결책

- 1 새로운 대기 노드를 배포합니다.
- 2 연결되지 않은 대기 노드를 등록 취소합니다.

다음에 수행할 작업

고가용성 클러스터에서 대기 셀 장애로부터 복구의 내용을 참조하십시오.

클러스터 상태가 SSH 문제를 나타냄

데이터베이스 HA 구성을 사용하는 VMware Cloud Director 장치 배포에서 **postgres** 사용자는 SSH를 통해 피어 데이터베이스 노드에 연결할 수 없습니다.

문제

데이터베이스 노드 간에 SSH 문제가 있는 경우 VMware Cloud Director에 localClusterHealth가 SSH_PROBLEM으로 표시됩니다. 심각한 문제는 가능한 한 빨리 해결해야 합니다.

localClusterHealth는 VMware Cloud Director 장치 관리 사용자 인터페이스를 사용하거나 /nodes VMware Cloud Director 장치 API를 실행하여 볼 수 있습니다. [VMware Cloud Director 장치 API](#) 설명서를 참조하십시오.

SSH 문제가 있는 피어 노드에서 /nodes API를 실행하면 /nodes API는 localClusterHealth가 SSH_PROBLEM이고 localClusterFailover가 INDETERMINATE라는 정보를 반환합니다. /nodes API를 실행하는 노드가 SSH를 통해 피어 노드 중 하나에 연결할 수 없기 때문에 페일오버 모드는 INDETERMINATE입니다. SSH 문제가 있는 노드에 대한 응답 본문의 "failover" 출력 부분에 있는 "details"에는 ssh failed. command: ssh unreachable_standby_host_IP /usr/bin/grep failover>manual /opt/vmware/vpostgres/10/etc/repmgr.conf가 표시됩니다.

예를 들어 대기 노드에 SSH 문제가 있고 GET https://primary_host_IP:5480/api/1.0.0/nodes를 실행하면 /nodes API는 다음 정보를 반환할 수 있습니다.

```
{
  "localClusterFailover": "INDETERMINATE",
  "localClusterHealth": "SSH_PROBLEM",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
```

```

        "repmgrd": {
            "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
            "status": "NOT APPLICABLE"
        }
    },
    "id": primary_node_ID,
    "location": "default",
    "name": "primary_host_name",
    "nodeHealth": "HEALTHY",
    "nodeRole": "PRIMARY",
    "role": "primary",
    "status": "* running",
    "upstream": ""
},
{
    "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
    "failover": {
        "details": "failover = manual",
        "mode": "MANUAL",
        "repmgrd": {
            "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = not applicable",
            "status": "NOT APPLICABLE"
        }
    },
    "id": running_standby_node_ID,
    "location": "default",
    "name": "running_standby_host_name",
    "nodeHealth": "HEALTHY",
    "nodeRole": "STANDBY",
    "role": "standby",
    "status": "running",
    "upstream": "primary_host_name"
},
{
    "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
    "failover": {
        "details": "ssh failed. command: ssh unreachable_standby_host_IP /usr/bin/
grep failover>manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
        "mode": "UNKNOWN",
        "repmgrd": {
            "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = not running",
            "status": "NOT RUNNING"
        }
    },
    "id": unreachable_standby_node_ID,
    "location": "default",
    "name": "unreachable_standby_host_name",
    "nodeHealth": "HEALTHY",
    "nodeRole": "STANDBY",
    "role": "standby",

```



```

        "status": "running",
        "upstream": "primary_host_name"
    }
],
"warnings": []
}

```

GET `https://unreachable_standby_host_IP:5480/api/1.0.0/nodes`를 실행하면, 노드를 신뢰할 수 없기 때문에 `localClusterFailover` 및 `localClusterState` 정보가 올바르지 않을 수 있습니다. `/nodes` API는 `unreachable_standby_host_name`이 피어 노드에 연결할 수 없다는 경고 메시지를 반환합니다. 예를 들어 `/nodes` API는 다음 정보를 반환할 수 있습니다.

```

{
  "localClusterFailover": "MANUAL",
  "localClusterHealth": "SSH_PROBLEM",
  "localClusterState": [
    {
      "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "ssh failed. command: ssh primary_host_IP /usr/bin/grep
failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
        "mode": "UNKNOWN",
        "repmgrd": {
          "details": "On node primary_node_ID (primary_host_name): repmgrd = n/a",
          "status": "UNKNOWN"
        }
      },
      "id": primary_node_ID,
      "location": "default",
      "name": "primary_host_name",
      "nodeHealth": "UNHEALTHY",
      "nodeRole": "PRIMARY",
      "role": "primary",
      "status": "? running",
      "upstream": ""
    },
    {
      "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
      "failover": {
        "details": "ssh failed. command: ssh running_standby_host_IP /usr/bin/grep
failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
        "mode": "UNKNOWN",
        "repmgrd": {
          "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = n/a",
          "status": "UNKNOWN"
        }
      },
      "id": running_standby_node_ID,
      "location": "default",
      "name": "running_standby_host_name",

```

```

        "nodeHealth": "UNHEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "? running",
        "upstream": "primary_host_name"
    },
    {
        "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
        "failover": {
            "details": "failover = manual",
            "mode": "MANUAL",
            "repmgrd": {
                "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = not applicable",
                "status": "NOT APPLICABLE"
            }
        },
        "id": unreachable_standby_node_ID,
        "location": "default",
        "name": "unreachable_standby_host_name",
        "nodeHealth": "HEALTHY",
        "nodeRole": "STANDBY",
        "role": "standby",
        "status": "running",
        "upstream": "? primary_host_name"
    }
],
"warnings": [
    "unable to connect to node \"primary_host_name\" (ID: primary_node_ID)",
    "unable to connect to node \"running_standby_host_name\" (ID:
running_standby_node_ID)",
    "unable to connect to node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID)'s upstream node \"primary_host_name\" (ID: primary_node_ID)",
    "unable to determine if node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID) is attached to its upstream node \"primary_host_name\" (ID:
primary_node_ID)"
]
}

```

원인

VMware Cloud Director는 **postgres** 사용자의 SSH 인증서를 NFS 공유 전송 서버 스토리지에 저장합니다. 모든 데이터베이스 노드는 공유 전송 서버 스토리지에 액세스할 수 있어야 합니다. 데이터베이스 노드를 신뢰할 수 없는 경우, 즉 **postgres** 사용자의 SSH 인증서가 더 이상 유효하지 않거나 액세스할 수 없는 경우, 해당 노드는 SSH 클라이언트를 사용하여 피어 노드에서 명령을 실행할 수 없습니다. VMware Cloud Director 장치가 HA 모드에서 제대로 작동하려면 이 기능이 있어야 합니다.

해결책

- 1 노드 간에 연결 문제가 있는지 확인한 후 문제를 해결하십시오. 데이터베이스고가용성 클러스터에서 연결 상태 확인의 내용을 참조하십시오.

- 2 다음 명령을 실행하여 SSH 문제가 있는 노드에서 appliance-sync.timer 서비스가 실행 중인지 확인합니다.

```
systemctl status appliance-sync.timer
```

예를 들어 명령이 다음을 반환할 수 있습니다.

```
* appliance-sync.timer - Periodic check and sync of needed files for Cloud Appliance
functionality
   Loaded: loaded (/lib/systemd/system/appliance-sync.timer; enabled; vendor preset:
enabled)
   Active: active (waiting) since Sat 2020-09-05 23:22:49 UTC; 1 months 9 days ago

Warning: Journal has been rotated since unit was started. Log output is incomplete or
unavailable.
```

- 3 appliance-sync.timer 서비스의 상태가 활성이 아니면 다음 명령을 실행하여 서비스를 다시 시작하십시오.

```
systemctl start appliance-sync.timer
```

- 4 약 90초 동안 기다렸다가 VMware Cloud Director 관리 UI를 사용하거나 /nodes API를 호출하여 클러스터 상태가 정상인지 확인합니다.

로그 파일을 사용하여 VMware Cloud Director 업데이트 및 패치 문제 해결

VMware Cloud Director 장치에 패치를 적용할 때 로그 파일에서 오류 및 경고를 검토할 수 있습니다.

문제

vamicli 명령이 오류를 반환하면 로그 파일을 사용하여 문제를 해결할 수 있습니다.

해결책

- 1 VMware Cloud Director 장치 콘솔에 **root**로 직접 로그인하거나 SSH를 통해 연결합니다.
- 2 적절한 로그 파일로 이동합니다.
 - vamicli update --check이 실패하면 /opt/vmware/var/log/vami/vami.log로 이동합니다.
 - vamicli update --install latest가 실패하면 /opt/vmware/var/log/vami/updatecli.log로 이동합니다.
- 3 로그 파일을 검토합니다.

VMware Cloud Director 업데이트 확인 실패

VMware Cloud Director 장치에 대한 업데이트를 확인할 때 vamicli update --check 명령을 실행하면 실패할 수도 있습니다.

문제

VMware Cloud Director 장치에 패치를 적용하는 절차 중에는 `vamcli update --check` 명령을 실행하여 사용 가능한 업데이트를 확인합니다. `vamcli update --check` 명령이 실패하고 다음 오류 메시지가 표시될 수 있습니다. `Failure: Error downloading manifest. Please contact your vendor.`

원인

업데이트 저장소 디렉토리에 대한 경로가 잘못되었습니다.

해결책

- 1 `vamcli` 명령을 올바른 경로와 함께 실행합니다.

```
vamcli update --repo file:/root/local-update-repo
```

- 2 명령을 다시 실행하여 업데이트를 확인합니다.

```
vamcli update --check
```

VMware Cloud Director의 최신 업데이트 설치 실패

VMware Cloud Director 장치에 최신 업데이트를 설치할 때 `vamcli update --install latest` 명령을 실행하면 실패할 수 있습니다.

문제

VMware Cloud Director 장치에 패치를 적용하는 절차 중에 `vamcli update --install latest` 명령을 실행하여 사용 가능한 최신 패치를 적용합니다. `vamcli update --install latest` 명령이 실패하고 다음 오류 메시지가 표시될 수 있습니다. `Failure: Error while running package installation`

원인

이 오류는 NFS 서버에 액세스할 수 없을 때 발생합니다.

해결책

- 1 `/opt/vmware/vcloud-director/data/transfer`에 마운트된 NFS 서버에 액세스할 수 있는지 확인합니다.
- 2 명령을 다시 실행하여 사용 가능한 패치를 적용합니다.

```
vamcli update --install latest
```

Linux에서 VMware Cloud Director 설치, 업그레이드 및 관리

4

하나 이상의 Linux 서버에 VMware Cloud Director 소프트웨어를 설치하거나 하나 이상의 VMware Cloud Director 장치 인스턴스를 배포하여 VMware Cloud Director 서버 그룹을 생성합니다. 설치 과정에서 네트워크 및 데이터베이스 연결 설정을 비롯한 초기 VMware Cloud Director 구성을 수행합니다.

Linux용 VMware Cloud Director 소프트웨어에는 외부 데이터베이스가 필요하지만, VMware Cloud Director 장치는 내장형 PostgreSQL 데이터베이스를 사용합니다.

VMware Cloud Director 서버 그룹을 생성한 후에 vSphere 리소스와 VMware Cloud Director 설치를 통합합니다. 네트워크 리소스의 경우 VMware Cloud Director는 NSX Data Center for vSphere, NSX-T Data Center 또는 둘 다를 사용할 수 있습니다.

기존 VMware Cloud Director 설치를 업그레이드하는 경우에는 VMware Cloud Director 소프트웨어 및 데이터베이스 스키마를 업데이트하고 서버, 데이터베이스 및 vSphere 간의 기존 관계는 그대로 유지합니다.

Linux의 기존 VMware Cloud Director 설치를 VMware Cloud Director 장치로 마이그레이션하는 경우, VMware Cloud Director 소프트웨어를 업데이트하고 데이터베이스를 장치의 내장형 데이터베이스로 마이그레이션합니다.

본 장은 다음 항목을 포함합니다.

- 구성 계획
- VMware Cloud Director 설치 준비
- Linux에 VMware Cloud Director 설치
- VMware Cloud Director 설치 후 작업
- Linux에서 VMware Cloud Director 업그레이드
- VMware Cloud Director 업그레이드 후 작업

구성 계획

vSphere는 VMware Cloud Director에 스토리지, 계산 및 네트워킹 용량을 제공합니다. 설치를 시작하기 전에 클라우드에 필요한 vSphere 및 VMware Cloud Director 용량을 고려하여 이를 지원할 수 있는 구성을 계획하십시오.

필요한 구성은 클라우드에 포함되어 있는 조직의 수, 각 조직의 사용자 수 및 해당 사용자의 활동 수준에 따라 달라집니다. 다음은 대부분의 구성 작업을 시작할 때 참고할 수 있는 지침입니다.

- 클라우드에서 액세스할 수 있게 설정할 각 vCenter Server 시스템에 VMware Cloud Director 셀 하나를 할당합니다.
- 모든 대상 VMware Cloud Director Linux 서버는 "VMware Cloud Director 릴리스 정보"에 설명되어 있는 메모리 및 스토리지에 대한 최소 요구 사항 이상을 충족해야 합니다.
- Linux에 VMware Cloud Director를 설치하려면 [Linux에서 VMware Cloud Director용 외부 PostgreSQL 데이터베이스 구성](#)의 설명에 따라 VMware Cloud Director 데이터베이스를 구성합니다.

VMware Cloud Director 설치 준비

Linux 서버에 VMware Cloud Director를 설치하기 전에 환경을 준비해야 합니다.

Linux에서 VMware Cloud Director용 외부 PostgreSQL 데이터베이스 구성

VMware Cloud Director 셀은 데이터베이스를 사용하여 공유 정보를 저장합니다. Linux에서 VMware Cloud Director를 설치하기 전에 PostgreSQL 데이터베이스 인스턴스를 설치 및 구성하고 VMware Cloud Director 데이터베이스 사용자 계정을 만들어야 합니다.

PostgreSQL 데이터베이스는 VMware Cloud Director와 함께 사용할 때 특정 구성 요구 사항이 있습니다.

VMware Cloud Director에서 사용할 별도의 전용 데이터베이스 스키마를 생성해야 합니다. VMware Cloud Director는 다른 VMware 제품과 데이터베이스 스키마를 공유할 수 없습니다.

VMware Cloud Director는 PostgreSQL 데이터베이스에 대한 SSL 연결을 지원합니다. 자동 네트워크 및 데이터베이스 연결 구성 중에 또는 VMware Cloud Director 서버 그룹을 만든 후에 PostgreSQL 데이터베이스에서 SSL을 사용하도록 설정할 수 있습니다. [자동 구성 참조](#) 및 [외부 PostgreSQL 데이터베이스에서 추가 구성 수행](#)의 내용을 참조하십시오.

참고 Linux의 VMware Cloud Director만 외부 데이터베이스를 사용합니다. VMware Cloud Director 장치는 내장된 PostgreSQL 데이터베이스를 사용합니다.

사전 요구 사항

지원되는 VMware Cloud Director 데이터베이스에 대한 자세한 내용은 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

PostgreSQL 명령, 스크립팅 및 작업에 익숙해야 합니다.

절차

1 데이터베이스 서버를 구성합니다.

일반적인 VMware Cloud Director 서버 그룹에는 16GB의 메모리, 100GB의 스토리지 및 4개의 CPU가 있는 데이터베이스 서버가 적합합니다.

2 데이터베이스 서버에 지원되는 PostgreSQL 배포를 설치합니다.

- 데이터베이스의 SERVER_ENCODING 값은 UTF-8이어야 합니다. 이 값은 데이터베이스를 설치할 때 설정되며 데이터베이스 서버 운영 체제에 사용되는 인코딩과 항상 일치합니다.
- PostgreSQL initdb 명령을 사용하여 LC_COLLATE 및 LC_CTYPE의 값을 en_US.UTF-8로 설정합니다. 예는 다음과 같습니다.

```
initdb --locale=en_US.UTF-8
```

3 데이터베이스 사용자를 만듭니다.

다음 명령은 vcloud라는 사용자를 만듭니다.

```
create user vcloud;
```

4 데이터베이스 인스턴스를 만들고 소유자에게 제공합니다.

다음과 같은 명령을 사용하여 이름이 vcloud인 데이터베이스 사용자를 데이터베이스 소유자로 지정합니다.

```
create database vcloud owner vcloud;
```

5 데이터베이스 소유자 계정에 데이터베이스 암호를 할당합니다.

다음 명령은 데이터베이스 소유자 vcloud에 암호 vcloudpass를 할당합니다.

```
alter user vcloud password 'vcloudpass';
```

6 데이터베이스 소유자가 데이터베이스에 로그인할 수 있도록 합니다.

다음 명령은 데이터베이스 소유자 vcloud에 login 옵션을 할당합니다.

```
alter role vcloud with login;
```

다음에 수행할 작업

VMware Cloud Director 서버 그룹을 만든 후에는 VMware Cloud Director 셸에서 SSL 연결을 요구하도록 PostgreSQL 데이터베이스를 구성하고 최적의 성능을 위해 일부 데이터베이스 매개 변수를 조정할 수 있습니다. 외부 PostgreSQL 데이터베이스에서 추가 구성 수행의 내용을 참조하십시오.

Linux에서 VMware Cloud Director를 위한 전송 서버 스토리지 준비

업로드/다운로드 항목 및 외부에서 게시 또는 구독되는 카탈로그 항목을 위한 임시 스토리지를 제공하려면 VMware Cloud Director 서버 그룹의 모든 서버가 NFS 또는 기타 공유 스토리지 볼륨에 액세스할 수 있도록 설정해야 합니다.

서버 그룹의 각 구성원은 이 볼륨을 동일한 마운트 지점(/opt/vmware/vcloud-director/data/transfer)에 마운트합니다. 이 볼륨의 공간은 다음과 같은 여러 가지 방식으로 사용됩니다.

- 전송하는 동안 업로드 및 다운로드가 이 스토리지를 차지합니다. 전송이 완료되면 업로드 및 다운로드가 스토리지에서 제거됩니다. 60분 동안 진행되지 않은 전송은 만료된 것으로 표시되고 시스템에 의해 정리됩니다. 전송되는 이미지가 클 수 있으므로 이 용도로 사용하려면 적어도 수백 기가바이트를 할당하는 것이 좋습니다.
- 외부에 게시되고 게시된 콘텐츠에 대한 캐싱을 사용할 수 있는 카탈로그의 카탈로그 항목은 이 스토리지를 차지합니다. 외부에 게시되지만 캐싱을 사용할 수 없는 카탈로그의 항목은 이 스토리지를 차지하지 않습니다. 클라우드의 조직에서 외부에 게시되는 카탈로그를 만들 수 있도록 설정하는 경우에는 수백 또는 수천 개의 카탈로그 항목이 이 볼륨의 공간을 필요로 한다고 가정할 수 있습니다. 각 카탈로그 항목의 크기는 압축된 OVF 형식의 가상 시스템 크기입니다.

참고 전송 서버 스토리지의 볼륨에는 향후 확장을 위한 용량이 있어야 합니다.

공유 스토리지 옵션

기존 Linux 기반 NFS 서버 또는 Microsoft Windows Server와 같은 기타 솔루션, VMware vSAN 파일 서비스 NFS 기능 등은 공유 스토리지를 제공할 수 있습니다. vSAN 7.0부터는 vSAN 파일 서비스 기능을 통해 NFS 3.0 및 NFS 4.1 프로토콜을 사용하여 NFS 공유를 내보낼 수 있습니다. vSAN 파일 서비스에 대한 자세한 내용은 [VMware vSphere 제품 설명서](#)의 "VMware vSAN 관리" 가이드를 참조하십시오.

NFS 서버 구성을 위한 요구 사항

NFS 서버 구성을 위해서는 VMware Cloud Director가 NFS 기반 전송 서버 스토리지 위치에 파일을 쓰고 읽을 수 있어야 한다는 구체적인 요구 사항이 있습니다. 이로 인해 **vcloud** 사용자는 표준 클라우드 운영을 수행할 수 있고 **root** 사용자는 다중 셀 로그 수집을 수행할 수 있습니다.

- NFS 서버의 내보내기 목록은 VMware Cloud Director 서버 그룹의 각 서버 멤버가 내보내기 목록에서 식별된 공유 위치에 대한 읽기/쓰기 액세스 권한을 갖도록 허용해야 합니다. 이 기능을 사용하면 **vcloud** 사용자가 공유 위치에 파일을 쓰고 읽을 수 있습니다.
- NFS 서버는 VMware Cloud Director 서버 그룹의 각 서버에서 **root** 계정으로 공유 위치에 대한 읽기/쓰기 액세스 권한을 허용해야 합니다. 이 기능을 사용하면 `vmware-vcd-support` 스크립트를 다중 셀 옵션과 함께 사용하여 단일 번들에서 모든 셀의 로그를 한 번에 수집할 수 있습니다. 이 공유 위치에 대한 NFS 내보내기 구성에서 `no_root_squash`를 사용하여 이 요구 사항을 충족할 수 있습니다.

Linux NFS 서버 예제

예를 들어, Linux NFS 서버에 VMware Cloud Director 서버 그룹의 전송 공간으로 vCDspace라는 디렉토리가 있고 해당 위치가 /nfs/vCDspace인 경우 이 디렉토리를 내보내려면 소유권과 사용 권한이

root:root 및 **750**이어야 합니다. vCD-Cell1-IP, vCD-Cell2-IP, vCD-Cell3-IP라는 3개 셀의 공유 위치에 대한 읽기/쓰기 액세스 권한을 허용하는 메서드는 no_root_squash 메서드입니다. /etc/exports 파일에 다음 줄을 추가해야 합니다.

```
/nfs/vCDspace vCD_Cell1_IP_Address(rw, sync, no_subtree_check, no_root_squash)
/nfs/vCDspace vCD_Cell2_IP_Address(rw, sync, no_subtree_check, no_root_squash)
/nfs/vCDspace vCD_Cell3_IP_Address(rw, sync, no_subtree_check, no_root_squash)
```

내보내기 줄에서 각 셀 IP 주소와 바로 다음 왼쪽 괄호 사이에 공백이 없어야 합니다. 셀이 공유 위치에 데이터를 쓰는 동안 NFS 서버가 재부팅되는 경우, 내보내기 구성에서 sync 옵션을 사용하면 공유 위치에서 데이터가 손상되지 않습니다. 내보내기 구성에서 no_subtree_check 옵션을 사용하면 파일 시스템의 하위 디렉토리를 내보낼 때 안정성이 향상됩니다.

VMware Cloud Director 서버 그룹의 각 서버에 대해 NFS 서버의 /etc/exports 파일에 해당 항목이 있어야 NFS 공유를 모두 마운트할 수 있습니다. NFS 서버에서 /etc/exports 파일을 변경한 후 exportfs -a를 실행하여 모든 NFS 공유를 다시 내보냅니다.

VMware Cloud Director 설치에 대한 최신 버전 업그레이드를 계획할 때 고려할 사항

VMware Cloud Director 서버 그룹을 업그레이드하는 동안 업그레이드된 버전에 대한 설치 파일을 실행하여 VMware Cloud Director 서버 그룹의 모든 멤버를 업그레이드합니다. 편의를 위해 일부 조직에서는 업그레이드용 설치 파일을 전송 서버 스토리지 위치로 다운로드하고 이 위치에서 파일을 실행하도록 합니다. 이렇게 하면 모든 셀이 해당 위치에 액세스할 수 있기 때문입니다. 업그레이드 설치 파일을 실행하는 데 **root** 사용자를 사용해야 하기 때문에 전송 서버 스토리지 위치를 사용하여 업그레이드를 실행하려면 업그레이드를 수행할 때 **root** 사용자가 업그레이드 설치 파일을 실행할 수 있는지 확인해야 합니다. **root** 사용자로 업그레이드를 실행할 수 없는 경우에는 **root** 사용자로 실행할 수 있는 다른 위치(예: NFS 마운트 외부의 다른 디렉토리)에 파일을 복사해야 합니다.

VMware 공용 키 다운로드 및 설치

설치 파일은 디지털로 서명됩니다. 서명을 확인하려면 VMware 공용 키를 다운로드하여 설치해야 합니다.

Linux rpm 도구와 VMware 공용 키를 사용하여 VMware Cloud Director 설치 파일이나 vmware.com에서 다운로드한 다른 모든 서명된 파일의 디지털 서명을 확인할 수 있습니다. VMware Cloud Director를 설치할 예정인 컴퓨터에 공용 키를 설치하면 설치 또는 업그레이드 작업의 일부로 디지털 서명이 확인됩니다. 설치나 업그레이드 절차를 시작하기 전에 수동으로 서명을 확인한 후 확인된 파일을 모든 설치 또는 업그레이드에 사용할 수도 있습니다.

참고 다운로드 사이트에는 다운로드의 체크섬 값이 함께 게시됩니다. 체크섬은 일반적으로 두 가지 형식으로 게시되는데, 체크섬을 확인하면 다운로드한 파일의 내용이 게시된 파일의 내용과 동일한지 확인할 수 있습니다. 체크섬은 디지털 서명을 확인하지 않습니다.

절차

- 1 VMware 패키징 공용 키를 저장할 디렉터리를 만듭니다.
- 2 웹 브라우저를 사용하여 <http://packages.vmware.com/tools/keys> 디렉터리에서 모든 VMware 공용 패키징 공용 키를 다운로드하십시오.
- 3 앞에서 만든 디렉터리에 키 파일을 저장합니다.
- 4 다운로드한 각 키에 대해 다음 명령을 실행하여 해당 키를 가져옵니다.

```
# rpm --import /key_path/key_name
```

*key_path*는 키가 저장된 디렉터리입니다.

*key_name*은 키의 파일 이름입니다.

VMware Cloud Director용 NSX Data Center for vSphere 설치 및 구성

VMware Cloud Director 설치 환경에서 NSX Data Center for vSphere의 네트워크 리소스를 사용하려는 경우, NSX Data Center for vSphere를 설치하여 구성하고 VMware Cloud Director 설치에 포함하려는 각 vCenter Server 인스턴스에 고유한 NSX Manager 인스턴스를 연결해야 합니다.

NSX Manager는 NSX Data Center for vSphere 다운로드에 포함되어 있습니다. VMware Cloud Director 및 기타 VMware 제품 간 호환성에 대한 최신 정보는 "VMware 제품 상호 운용성 매트릭스" (<http://partnerware>)를 참조하십시오. 네트워크 요구 사항에 대한 자세한 내용은 [VMware Cloud Director에 대한 네트워크 구성 요구 사항](#)을 참조하십시오.

중요 VMware Cloud Director를 새로 설치할 경우에만 이 절차가 적용됩니다. VMware Cloud Director의 기존 설치를 업그레이드할 경우 [Linux에서 VMware Cloud Director 업그레이드](#)를 참조하십시오.

사전 요구 사항

각 vCenter Server 시스템이 NSX Manager 설치를 위한 전제 조건을 충족하는지 확인합니다.

절차

- 1 NSX Manager 가상 장치에 대한 설치 작업을 수행합니다.
"NSX 설치 가이드"를 참조하십시오.
- 2 설치한 NSX Manager 가상 장치에 로그인하여 설치 중에 지정한 설정을 확인합니다.
- 3 설치한 NSX Manager 가상 장치를 계획한 VMware Cloud Director 설치에서 VMware Cloud Director에 추가하려는 vCenter Server 시스템과 연결합니다.
- 4 연결된 NSX Manager 인스턴스에서 VXLAN 지원을 구성합니다.

VMware Cloud Director에서는 VXLAN 네트워크 풀을 생성하여 제공자 VDC에 네트워크 리소스를 제공합니다. 연결된 NSX Manager에 VXLAN 지원이 구성되지 않은 경우 제공자 VDC에서 네트워크 풀 오류를 표시하고 사용자는 다른 유형의 네트워크 풀을 만들어 제공자 VDC와 연결해야 합니다. VXLAN 지원 구성에 대한 자세한 내용은 "NSX 관리 가이드"의 내용을 참조하십시오.

- 5 (선택 사항) 시스템의 Edge 게이트웨이가 분산 라우팅을 제공하도록 하려면 NSX Controller 클러스터를 설정합니다.

"NSX 관리 가이드"를 참조하십시오.

VMware Cloud Director용 NSX-T Data Center 설치 및 구성

VMware Cloud Director 설치 환경에서 NSX-T Data Center의 네트워크 리소스를 사용하려는 경우, NSX-T Data Center를 설치하고 구성해야 합니다.

중요 NSX-T Data Center 개체 및 도구를 구성하려면 간소화된 정책 UI 및 간소화된 UI에 해당하는 정책 API를 사용합니다. 자세한 내용은 "NSX-T Data Center 관리 가이드"에서 NSX-T Manager 개요를 참조하십시오.

VMware Cloud Director와 기타 VMware 제품 간 호환성에 대한 최신 정보는 [VMware 제품 상호 운용성 매트릭스](#)를 참조하십시오.

네트워크 요구 사항에 대한 자세한 내용은 [VMware Cloud Director에 대한 네트워크 구성 요구 사항](#)을 참조하십시오.

VMware Cloud Director를 새로 설치할 경우에만 이 절차가 적용됩니다. VMware Cloud Director의 기존 설치를 업그레이드할 경우 [Linux에서 VMware Cloud Director 업그레이드](#)를 참조하십시오.

사전 요구 사항

NSX-T Data Center를 숙지합니다.

절차

- 1 NSX-T Manager 가상 장치를 배포하고 구성합니다.

NSX-T Manager 배포에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드" 항목을 참조하십시오.

- 2 네트워킹 요구 사항을 기반으로 전송 영역을 생성합니다.

전송 영역 생성에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드" 항목을 참조하십시오.

참고

- 3 Edge 노드 및 Edge 클러스터를 배포하고 구성합니다.

NSX Edge 생성에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드" 항목을 참조하십시오.

- 4 ESXi 호스트 전송 노드를 구성합니다.

관리되는 호스트 전송 노드 구성에 대한 자세한 내용은 "NSX-T Data Center 설치 가이드" 항목을 참조하십시오.

- 5 Tier-0 게이트웨이를 생성합니다.

Tier-0 생성에 대한 자세한 내용은 "NSX-T Data Center 관리 가이드" 항목을 참조하십시오.

다음에 수행할 작업

VMware Cloud Director를 설치한 후 다음을 수행할 수 있습니다.

- 1 클라우드에 NSX-T Manager 인스턴스를 등록합니다.

NSX-T Manager 인스턴스 등록에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드" 항목을 참조하십시오.

- 2 NSX-T Data Center 전송 영역에서 지원하는 네트워크 풀을 생성합니다.

NSX-T Data Center 전송 영역에서 지원하는 네트워크 풀을 생성하는 방법에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드" 항목을 참조하십시오.

- 3 Tier-0 게이트웨이를 외부 네트워크로 가져옵니다.

NSX-T Data Center Tier-0 논리적 라우터가 지원하는 외부 네트워크를 추가하는 방법에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드" 항목을 참조하십시오.

Linux에 VMware Cloud Director 설치

하나 이상의 Linux 서버에 VMware Cloud Director 소프트웨어를 설치하여 VMware Cloud Director 서버 그룹을 만들 수 있습니다. 첫 번째 그룹 구성원을 설치 및 구성하면 그룹의 추가 구성원을 구성하는 데 사용하는 지시 파일을 만들어집니다.

이 절차는 새 설치에만 적용됩니다. 기존의 VMware Cloud Director 설치를 업그레이드할 경우 [Linux에서 VMware Cloud Director 업그레이드](#)의 내용을 참조하십시오.

중요 하나의 서버 그룹에서 Linux에 설치된 VMware Cloud Director 및 VMware Cloud Director 장치 배포의 혼합은 지원되지 않습니다.

버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)의 내용을 참조하십시오.

사전 요구 사항

- 서버 그룹에 대한 대상 서버가 [장 2 VMware Cloud Director 하드웨어 및 소프트웨어 요구 사항](#)을 충족하는지 확인합니다.
- 서버 그룹에 대한 대상 서버의 각 끝점에 대한 SSL 인증서를 생성했는지 확인합니다. SSL 인증서에 대한 경로 이름의 모든 디렉터리는 모든 사용자가 읽을 수 있어야 합니다. 서버 그룹의 모든 구성원에 동일한 키 저장소 경로(예: /tmp/certificates.ks)를 사용하면 설치 프로세스가 간소화됩니다. [Linux용 VMware Cloud Director에 대한 SSL 인증서를 만들기 전에](#)의 내용을 참조하십시오.

- VMware Cloud Director 서버 그룹의 모든 대상 서버에서 액세스할 수 있는 NFS 또는 기타 공유 스토리지 볼륨을 준비했는지 확인합니다. [Linux에서 VMware Cloud Director를 위한 전송 서버 스토리지 준비](#)의 내용을 참조하십시오.
- 그룹의 모든 서버에서 액세스할 수 있는 VMware Cloud Director 데이터베이스를 생성했는지 확인합니다. [Linux에서 VMware Cloud Director용 외부 PostgreSQL 데이터베이스 구성](#)의 내용을 참조하십시오. 데이터베이스 서버를 재부팅하면 데이터베이스 서비스가 시작되는지 확인합니다.
- [VMware Cloud Director에 대한 네트워크 구성 요구 사항](#)에 설명된 대로 모든 VMware Cloud Director 서버, 데이터베이스 서버, 모든 vCenter Server 시스템 및 연결된 NSX Manager 인스턴스에서 환경의 각 호스트 이름을 확인할 수 있는지 확인합니다.
- 모든 VMware Cloud Director 서버와 데이터베이스 서버가 [VMware Cloud Director에 대한 네트워크 구성 요구 사항](#)에 나와 있는 허용치 내에서 네트워크 시간 서버와 동기화되는지 확인합니다.
- LDAP 서비스로부터 사용자나 그룹을 가져올 계획이 있는 경우, 각 VMware Cloud Director 서버가 해당 서비스에 액세스할 수 있는지 확인합니다.
- [네트워크 보안 요구 사항](#)에 나와 있는 대로 방화벽 포트를 엽니다. VMware Cloud Director와 vCenter Server 시스템 사이에는 포트 443을 열어 두어야 합니다.

절차

1 서버 그룹의 첫 번째 구성원에 VMware Cloud Director 설치

환경을 준비하고 전제 조건을 확인한 다음, 첫 번째 대상 Linux 서버에서 VMware Cloud Director 설치 관리자를 실행하여 VMware Cloud Director 서버 그룹 생성을 시작할 수 있습니다.

2 Linux에 VMware Cloud Director에 대한 SSL 인증서 생성 및 관리

VMware Cloud Director는 SSL을 사용하여 클라이언트와 서버 간 통신 보안을 유지합니다. 각 VMware Cloud Director 서버는 HTTPS용과 콘솔 프록시 통신용으로 서로 다른 두 가지 SSL 끝점을 지원해야 합니다.

3 네트워크 및 데이터베이스 연결 구성

서버 그룹의 첫 번째 구성원에 VMware Cloud Director를 설치한 후 이 셀에 대한 네트워크 및 데이터베이스 연결을 생성하는 구성 스크립트를 실행해야 합니다. 스크립트는 서버 그룹의 추가 구성원을 구성할 때 사용해야 하는 지시 파일을 생성합니다.

4 서버 그룹의 추가 구성원에 VMware Cloud Director 설치

언제든지 VMware Cloud Director 서버 그룹에 서버를 추가할 수 있습니다. 서버 그룹에 속한 모든 서버는 동일한 데이터베이스 연결 정보를 사용하여 구성되어야 하므로 그룹의 첫 번째 구성원을 구성할 때 만든 지시 파일을 사용해야 합니다.

다음에 수행할 작업

셀 관리 도구의 `system-setup` 명령을 사용하여 시스템 관리자 계정 및 관련 정보로 서버 그룹의 데이터베이스를 초기화합니다. [VMware Cloud Director 설치 구성](#)의 내용을 참조하십시오.

서버 그룹의 첫 번째 구성원에 VMware Cloud Director 설치

환경을 준비하고 전제 조건을 확인한 다음, 첫 번째 대상 Linux 서버에서 VMware Cloud Director 설치 관리자를 실행하여 VMware Cloud Director 서버 그룹 생성을 시작할 수 있습니다.

Linux용 VMware Cloud Director는 `vmware-vcloud-director-distribution-v.v.v-
"nnnnnn".bin` 형식의 이름을 가지는 디지털 서명된 실행 파일로 배포됩니다. 여기서 `v.v.v`는 제품 버전을 나타내고 `"nnnnnn"`은 빌드 번호를 나타냅니다. 예를 들면 `vmware-vcloud-director-distribution-8.10.0-3698331.bin`과 같습니다. 이 실행 파일을 실행하면 VMware Cloud Director가 설치 또는 업그레이드됩니다.

VMware Cloud Director 설치 관리자는 대상 서버가 모든 플랫폼 전제 조건을 충족하는지 확인한 후 해당 플랫폼에 VMware Cloud Director 소프트웨어를 설치합니다.

사전 요구 사항

- 대상 서버에 대한 슈퍼 사용자 자격 증명이 있는지 확인합니다.
- 설치 관리자에서 설치 파일의 디지털 서명을 확인하려면 대상 서버에 **VMware** 공용 키를 다운로드하여 설치합니다. 설치 파일의 디지털 서명을 이미 확인한 경우 설치 중에 다시 확인할 필요가 없습니다. [VMware 공용 키 다운로드 및 설치](#)의 내용을 참조하십시오.

절차

- 1 대상 서버에 **root**로 로그인합니다.

- 2 설치 파일을 대상 서버에 다운로드합니다.

미디어에 있는 소프트웨어를 구입한 경우에는 대상 서버가 액세스할 수 있는 위치에 설치 파일을 복사하십시오.

- 3 다운로드의 체크섬이 다운로드 페이지에 게시된 체크섬과 일치하는지 확인합니다.

MD5 및 SHA1의 체크섬 값이 다운로드 페이지에 게시되어 있습니다. 적절한 도구를 사용하여 다운로드한 설치 파일의 체크섬이 다운로드 페이지에 표시된 체크섬과 일치하는지 확인합니다. 다음 형식의 Linux 명령은 *installation-file*에 대한 체크섬을 표시합니다.

```
[root@cell11 /tmp]# md5sum installation-file
```

이 명령은 설치 파일 체크섬을 반환하며, 이 값은 다운로드 페이지의 MD5 체크섬과 일치해야 합니다.

- 4 설치 파일을 실행할 수 있는지 확인합니다.

설치 파일은 **실행** 권한이 있어야 실행할 수 있습니다. 이 권한이 있는지 확인하려면 콘솔, 셸 또는 터미널 창을 열고 다음 Linux 명령을 실행합니다. 명령에서 *installation-file*은 VMware Cloud Director 설치 파일의 전체 경로 이름입니다.

```
[root@cell11 /tmp]# chmod u+x installation-file
```

5 설치 파일을 실행합니다.

설치 파일을 실행하려면 다음과 같이 전체 경로 이름을 입력합니다.

```
[root@cell11 /tmp]# ./installation-file
```

이 파일에는 설치 스크립트와 내장된 RPM 패키지가 포함되어 있습니다.

참고 공백이 포함된 디렉터리가 해당 경로 이름에 있는 설치 파일은 실행할 수 없습니다.

대상 서버에 VMware 공용 키를 설치하지 않은 경우에는 설치 관리자에 다음과 같은 형식의 경고가 출력됩니다.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

설치 관리자는 다음 작업을 수행합니다.

- a 호스트가 모든 요구 사항을 충족하는지 확인합니다.
- b 설치 파일의 디지털 서명을 확인합니다.
- c vcloud 사용자 및 그룹을 만듭니다.
- d VMware Cloud Director RPM 패키지의 압축을 풉니다.
- e 소프트웨어를 설치합니다.

설치가 끝나면, 네트워크 및 데이터베이스 연결을 구성하는 구성 스크립트를 실행하라는 메시지가 설치 관리자에 표시됩니다.

6 구성 스크립트를 실행할지 여부를 선택합니다.

- a 대화형 모드에서 구성 스크립트를 실행하려면 **y**를 입력하고 Enter 키를 누릅니다.
- b 나중에 대화형 모드 또는 자동 모드에서 구성 스크립트를 실행하려면 **n**을 입력하고 Enter 키를 누릅니다.

Linux에 VMware Cloud Director에 대한 SSL 인증서 생성 및 관리

VMware Cloud Director는 SSL을 사용하여 클라이언트와 서버 간 통신 보안을 유지합니다. 각 VMware Cloud Director 서버는 HTTPS용과 콘솔 프록시 통신용으로 서로 다른 두 가지 SSL 끝점을 지원해야 합니다.

이 끝점은 별도의 IP 주소이거나 두 개의 서로 다른 포트를 사용하는 단일 IP 주소일 수 있습니다. 끝점마다 고유한 SSL 인증서가 필요합니다. 예를 들어 와일드카드 인증서를 사용하여 두 끝점에 동일한 인증서를 사용할 수 있습니다.

Linux용 VMware Cloud Director에 대한 SSL 인증서를 만들기 전에

Linux용 VMware Cloud Director를 설치하는 경우 서버 그룹의 각 구성원에 대해 2개의 인증서를 만든 후 호스트 키 저장소로 인증서를 가져와야 합니다.

참고 Linux용 VMware Cloud Director를 설치한 후에만 서버 그룹 구성원에 대한 인증서를 생성해야 합니다. VMware Cloud Director 장치는 첫 번째 부팅 중에 자체 서명된 SSL 인증서를 생성합니다.

절차

1 VMware Cloud Director 서버에 **root**로 로그인합니다.

2 이 서버의 IP 주소를 나열합니다.

`ifconfig` 같은 명령을 사용하여 이 서버의 IP 주소를 검색합니다.

3 각 IP 주소에 대해 다음 명령을 실행하여 해당 IP 주소가 바인딩되어 있는 FQDN(정규화된 도메인 이름)을 검색합니다.

```
nslookup ip-address
```

4 각 IP 주소 및 이와 연결된 FQDN을 기록해 둡니다. 두 서비스에 대해 단일 IP 주소를 사용하지 않는 경우 HTTPS 서비스에 대한 IP 주소와 콘솔 프록시 서비스에 대한 IP 주소를 결정합니다.

인증서를 생성할 때 FQDN을 제공해야 하고 네트워크 및 데이터베이스 연결을 구성할 때 IP 주소를 제공해야 합니다. IP 주소에 연결할 수 있는 다른 FQDN을 기록해 둡니다. 인증서에 주체 대체 이름을 포함하려는 경우 제공해야 하기 때문입니다.

다음에 수행할 작업

두 끝점에 대한 인증서를 만듭니다. 신뢰할 수 있는 CA(인증 기관)에서 서명한 인증서나 자체 서명된 인증서를 사용할 수 있습니다.

참고 CA 서명된 인증서의 신뢰 수준이 가장 높습니다.

- CA 서명된 SSL 인증서 만들기 및 가져오기에 대한 자세한 내용은 [Linux에 VMware Cloud Director에 대한 CA 서명된 SSL 인증서 키 저장소 생성](#) 항목을 참조하십시오.
- 자체 서명된 SSL 인증서 생성에 대한 자세한 내용은 [Linux에 VMware Cloud Director에 대한 자체 서명된 SSL 인증서 생성](#)의 내용을 참조하십시오.
- 개인 키 및 CA 서명된 인증서 파일을 가져오는 방법에 대한 자세한 내용은 [가져온 개인 키로 Linux용 VMware Cloud Director에 대한 CA 서명된 SSL 인증서 키 저장소 만들기](#)를 참조하십시오.

Linux에 VMware Cloud Director에 대한 자체 서명된 SSL 인증서 생성

자체 서명된 인증서는 신뢰도 문제가 거의 없는 환경에서 VMware Cloud Director의 SSL을 구성할 때 사용하면 편리합니다.

각 VMware Cloud Director 서버에는 HTTPS 서비스용과 콘솔 프록시 서비스용으로 각각 하나씩 JCEKS 키 저장소 파일에 두 개의 SSL 인증서가 필요합니다.

cell-management-tool을 사용하여 자체 서명된 SSL 인증서를 만듭니다. cell-management-tool 유틸리티는 구성 에이전트가 실행되기 전과 설치 파일을 실행한 후에 셀에 설치됩니다. 서버 그룹의 첫 번째 구성원에 [VMware Cloud Director 설치](#)의 내용을 참조하십시오.

중요 이 예제에서는 2,048비트 키 크기를 지정하지만, 적절한 키 크기를 선택하려면 설치 환경의 보안 요구 사항을 평가해야 합니다. 1,024비트보다 작은 키 크기는 NIST Special Publication 800-131A에 따라 더 이상 지원되지 않습니다.

절차

- 1 VMware Cloud Director 서버의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 명령을 실행하여 HTTPS 서비스 및 콘솔 프록시 서비스에 대한 공개 및 개인 키 쌍을 생성합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o
certificates.ks -w passwd
```

이 명령은 certificates.ks에 암호 passwd가 있는 키 저장소를 만들거나 업데이트합니다. cell-management-tool은 명령의 기본값을 사용하여 인증서를 생성합니다. 환경의 DNS 구성에 따라 발급자 CN은 각 서비스의 IP 주소 또는 FQDN으로 설정됩니다. 인증서는 기본 2048비트 키 길이를 사용하고, 만든 지 1년 후에 만료됩니다.

중요 키 저장소 파일과 이 파일이 저장된 디렉토리를 **vcloud.vcloud** 사용자가 읽을 수 있어야 합니다. VMware Cloud Director 설치 관리자가 이 사용자와 그룹을 만듭니다.

다음에 수행할 작업

키 저장소 경로 이름을 기록해 둡니다. 키 저장소 경로 이름은 VMware Cloud Director 셀에 대한 네트워크 및 데이터베이스 연결을 생성하기 위해 구성 스크립트를 실행할 때 필요합니다. [네트워크 및 데이터베이스 연결 구성](#)의 내용을 참조하십시오.

Linux에 VMware Cloud Director에 대한 CA 서명된 SSL 인증서 키 저장소 생성

CA 서명된 인증서를 생성하고 가져오면 SSL 통신에 대해 최고 수준의 신뢰를 제공하고 클라우드 인프라 내의 연결을 보호할 수 있습니다.

각 VMware Cloud Director 서버에는 클라이언트와 서버 간의 통신 보안을 위해 두 개의 SSL 인증서가 필요합니다. 각 VMware Cloud Director 서버는 HTTPS용과 콘솔 프록시 통신용으로 서로 다른 두 가지 SSL 끝점을 지원해야 합니다.

이 두 끝점은 별도의 IP 주소이거나 두 개의 서로 다른 포트를 사용하는 단일 IP 주소일 수 있습니다. 끝점마다 고유한 SSL 인증서가 필요합니다. 예를 들어 와일드카드 인증서를 사용하여 두 끝점에 동일한 인증서를 사용할 수 있습니다.

두 끝점 모두의 인증서에는 X.500 고유 이름과 X.509 주체 대체 이름 확장이 포함되어야 합니다.

신뢰할 수 있는 CA(인증 기관)에서 서명한 인증서나 자체 서명된 인증서를 사용할 수 있습니다.

cell-management-tool을 사용하여 자체 서명된 SSL 인증서를 만듭니다. cell-management-tool 유틸리티는 구성 에이전트가 실행되기 전과 설치 파일을 실행한 후에 셀에 설치됩니다. 서버 그룹의 첫 번째 구성원에 **VMware Cloud Director 설치**의 내용을 참조하십시오.

자체 개인 키와 CA 서명 인증서 파일이 이미 있는 경우 가져온 개인 키로 **Linux용 VMware Cloud Director에 대한 CA 서명된 SSL 인증서 키 저장소 만들기**에 설명된 절차를 따르십시오.

중요 이 예제에서는 2,048비트 키 크기를 지정하지만, 적절한 키 크기를 선택하려면 설치 환경의 보안 요구 사항을 평가해야 합니다. 1,024비트보다 작은 키 크기는 NIST Special Publication 800-131A에 따라 더 이상 지원되지 않습니다.

사전 요구 사항

- Java 버전 8 이상의 런타임 환경이 설치된 컴퓨터에 액세스할 수 있는지 확인하십시오. 그래야 keytool 명령을 사용하여 인증서를 가져올 수 있습니다. VMware Cloud Director 설치 관리자가 keytool의 복사본을 /opt/vmware/vcloud-director/jre/bin/keytool에 배치하지만, Java 런타임 환경이 설치된 모든 컴퓨터에서 이 절차를 수행할 수 있습니다. 다른 소스에서 keytool을 사용하여 만든 인증서는 VMware Cloud Director와 사용하도록 지원되지 않습니다. 이 명령줄 예제에서는 keytool이 사용자 경로에 있는 것으로 가정합니다.
- keytool 명령을 숙지합니다.
- generate-certs 명령에 사용할 수 있는 옵션에 대한 자세한 내용은 [HTTPS 및 콘솔 프록시 끝점에 대한 자체 서명된 인증서 생성](#)을 참조하십시오.
- certificates 명령에 사용할 수 있는 옵션에 대한 자세한 내용은 [HTTPS 및 콘솔 프록시 끝점에 대한 인증서 바꾸기](#) 항목을 참조하십시오.

절차

- 1 VMware Cloud Director 서버 셀의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 명령을 실행하여 HTTPS 서비스 및 콘솔 프록시 서비스에 대한 공개 및 개인 키 쌍을 생성합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o
certificates.ks -w keystore_password
```

이 명령은 certificates.ks에 지정된 암호가 있는 키 저장소를 만들거나 업데이트합니다. 인증서는 명령의 기본값을 사용하여 만들어집니다. 환경의 DNS 구성에 따라 발급자 CN은 각 서비스의 IP 주소 또는 FQDN으로 설정됩니다. 인증서는 기본 2048비트 키 길이를 사용하고, 만든 지 1년 후에 만료됩니다.

중요 키 저장소 파일과 이 파일이 저장된 디렉토리를 **vcloud.vcloud** 사용자가 읽을 수 있어야 합니다. VMware Cloud Director 설치 관리자가 이 사용자와 그룹을 만듭니다.

3 HTTPS 서비스 및 콘솔 프록시 서비스에 대한 인증서 서명 요청을 생성합니다.

중요 HTTPS 서비스와 콘솔 프록시 서비스에 대해 별도의 IP 주소를 사용 중인 경우 다음 명령에서 호스트 이름과 IP 주소를 조정합니다.

- a 인증서 서명 요청을 `http.csr` 파일에 만듭니다.

```
keytool -keystore certificates.ks -storetype PKCS12 -storepass keystore_password
-certreq -alias http -file http.csr -ext
"san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

- b 인증서 서명 요청을 `consoleproxy.csr` 파일에 만듭니다.

```
keytool -keystore certificates.ks -storetype PKCS12 -storepass keystore_password
-certreq -alias consoleproxy -file consoleproxy.csr -ext
"san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

4 인증서 서명 요청을 인증 기관에 보냅니다.

인증 기관이 웹 서버 유형을 지정하도록 요구하는 경우 Jakarta Tomcat을 사용합니다.

CA 서명된 인증서를 가져옵니다.

5 서명된 인증서를 PKCS12 키 저장소로 가져옵니다

- a CA(인증 기관)의 루트 인증서를 `root.cer` 파일에서 `certificates.ks` 키 저장소 파일로 가져옵니다.

```
keytool -import -storetype PKCS12 -storepass keystore_password -keystore
certificates.ks -alias root -file root_certificate_file
```

- b 중간 인증서 파일을 받은 경우 `intermediate.cer` 파일에서 `certificates.ks` 키 저장소 파일로 가져옵니다.

```
keytool -import -storetype PKCS12 -storepass keystore_password -keystore
certificates.ks -alias intermediate -file intermediate_certificate_file
```

- c HTTPS 서비스 인증서를 가져옵니다.

```
keytool -import -storetype PKCS12 -storepass keystore_password -keystore
certificates.ks -alias http -file http_certificate_file
```

- d 콘솔 프록시 서비스 인증서를 가져옵니다.

```
keytool -import -storetype PKCS12 -storepass keystore_password -keystore
certificates.ks -alias consoleproxy -file console_proxy_certificate_file
```

이러한 명령은 `certificates.ks` 파일을 새로 획득된 CA 서명된 인증서 버전으로 덮어씁니다.

- 6 인증서를 PKCS12 키 저장소로 가져왔는지 확인하려면 명령을 실행하여 키 저장소 파일의 콘텐츠를 나열합니다.

```
keytool -storetype PKCS12 -storepass keystore_password -keystore certificates.ks -list
```

- 7 서버 그룹의 모든 VMware Cloud Director 서버에서 이 절차를 반복하십시오.

다음에 수행할 작업

- VMware Cloud Director 인스턴스를 아직 구성하지 않은 경우 `configure` 스크립트를 실행하여 인증서 키 저장소를 VMware Cloud Director로 가져옵니다. [네트워크 및 데이터베이스 연결 구성](#)의 내용을 참조하십시오.

참고 FQDN(정규화된 도메인 이름) 및 연결된 IP 주소 목록을 생성한 서버가 아닌 다른 컴퓨터에 `certificates.ks` 키 저장소 파일을 만든 경우에는 키 저장소 파일을 해당 서버에 지금 복사합니다. 키 저장소 경로 이름은 구성 스크립트를 실행할 때 필요합니다.

- VMware Cloud Director 인스턴스를 이미 설치하고 구성한 경우 셀 관리 도구의 `certificates` 명령을 사용하여 인증서 키 저장소를 가져옵니다. [HTTPS 및 콘솔 프록시 끝점에 대한 인증서 바꾸기](#)의 내용을 참조하십시오.

가져온 개인 키로 Linux용 VMware Cloud Director에 대한 CA 서명된 SSL 인증서 키 저장소 만들기

자체 개인 키 및 CA 서명 인증서 파일이 있는 경우 VMware Cloud Director 환경에 키 저장소를 가져오기 전에 HTTPS와 콘솔 프록시 서비스 모두에 대한 인증서 및 개인 키를 가져올 키 저장소 파일을 생성해야 합니다.

사전 요구 사항

- [Linux용 VMware Cloud Director에 대한 SSL 인증서를 만들기 전에](#)의 내용을 참조하십시오.
- Java 버전 8 이상의 런타임 환경이 설치된 컴퓨터에 액세스할 수 있는지 확인하십시오. 그래야 `keytool` 명령을 사용하여 인증서를 가져올 수 있습니다. VMware Cloud Director 설치 관리자가 `keytool`의 복사본을 `/opt/vmware/vcloud-director/jre/bin/keytool`에 배치하지만, Java 런타임 환경이 설치된 모든 컴퓨터에서 이 절차를 수행할 수 있습니다. 다른 소스에서 `keytool`을 사용하여 만든 인증서는 VMware Cloud Director와 사용하도록 지원되지 않습니다. 이 명령줄 예제에서는 `keytool`이 사용자 경로에 있는 것으로 가정합니다.
- `keytool` 명령을 숙지합니다.
- OpenSSL을 다운로드하여 설치합니다.
- `certificates` 명령에 사용할 수 있는 옵션에 대한 자세한 내용은 [HTTPS 및 콘솔 프록시 끝점에 대한 인증서 바꾸기](#) 항목을 참조하십시오.

절차

- 1 중간 인증서가 있는 경우 명령을 실행하여 루트 CA 서명 인증서를 중간 인증서와 결합하고 인증서 체인을 생성합니다.

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```

- 2 OpenSSL을 사용하여 개인 키, 인증서 체인 및 해당 별칭으로 HTTPS와 콘솔 프록시 서비스 모두에 대한 중간 PKCS12 키 저장소 파일을 생성하고 각 키 저장소 파일에 대한 암호를 지정합니다.

- a HTTPS 서비스에 대한 키 저장소 파일을 생성합니다.

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http -passout pass:keystore_password -out http.p12 -chain
```

- b 콘솔 프록시 서비스에 대한 키 저장소 파일을 생성합니다.

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt -name consoleproxy -passout pass:keystore_password -out consoleproxy.p12 -chain
```

- 3 keytool을 사용하여 PKCS12 키 저장소를 certificate.ks 키 저장소로 가져옵니다.

- a 명령을 실행하여 HTTPS 서비스에 대한 PKCS12 키 저장소를 가져옵니다.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype PKCS12 -srckeystore http.p12 -srcstoretype PKCS12 -srcstorepass keystore_password
```

- b 명령을 실행하여 콘솔 프록시 서비스에 대한 PKCS12 키 저장소를 가져옵니다.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks -deststoretype PKCS12 -srckeystore consoleproxy.p12 -srcstoretype PKCS12 -srcstorepass keystore_password
```

- 4 인증서를 키 저장소로 가져왔는지 확인하려면 명령을 실행하여 키 저장소 파일의 콘텐츠를 나열합니다.

```
keytool -storetype PKCS12 -storepass keystore_password -keystore certificates.ks -list
```

- 5 환경의 모든 VMware Cloud Director 셸에 대해 이 절차를 반복합니다.

다음에 수행할 작업

- VMware Cloud Director 인스턴스를 아직 구성하지 않은 경우 configure 스크립트를 실행하여 인증서 키 저장소를 VMware Cloud Director로 가져옵니다. [네트워크 및 데이터베이스 연결 구성](#)의 내용을 참조하십시오.

참고 FQDN(정규화된 도메인 이름) 및 연결된 IP 주소 목록을 생성한 서버가 아닌 다른 컴퓨터에 certificates.ks 키 저장소 파일을 생성한 경우에는 키 저장소 파일을 해당 서버에 복사합니다. 키 저장소 경로 이름은 구성 스크립트를 실행할 때 필요합니다.

- VMware Cloud Director 인스턴스를 이미 설치하고 구성한 경우 셀 관리 도구의 `certificates` 명령을 사용하여 인증서 키 저장소를 가져옵니다. [HTTPS 및 콘솔 프록시 끝점에 대한 인증서 바꾸기](#)의 내용을 참조하십시오.

네트워크 및 데이터베이스 연결 구성

서버 그룹의 첫 번째 구성원에 VMware Cloud Director를 설치한 후 이 셀에 대한 네트워크 및 데이터베이스 연결을 생성하는 구성 스크립트를 실행해야 합니다. 스크립트는 서버 그룹의 추가 구성원을 구성할 때 사용해야 하는 지시 파일을 생성합니다.

VMware Cloud Director 서버 그룹의 모든 구성원은 데이터베이스 연결 및 기타 구성 정보를 공유합니다. VMware Cloud Director 서버 그룹의 첫 번째 구성원에서 구성 스크립트를 실행하면 스크립트는 이후의 서버 설치에 사용할 수 있도록 데이터베이스 연결 정보를 보존하는 지시 파일을 생성합니다.

대화형 모드 또는 자동 모드에서 구성 스크립트를 실행할 수 있습니다. 대화형 구성의 경우 옵션 없이 명령을 실행하고 필요한 설치 정보를 묻는 메시지가 스크립트에 표시됩니다. 자동 구성의 경우 명령 옵션을 사용하여 설치 정보를 입력합니다.

HTTPS 서비스 및 콘솔 프록시 서비스에 대해 서로 다른 두 개의 포트가 있는 단일 IP 주소를 사용하려는 경우에는 자동 모드에서 구성 스크립트를 실행해야 합니다.

참고 셀 관리 도구는 처음에 구성한 네트워크 및 데이터베이스 연결 세부 정보를 변경하는 데 사용할 수 있는 하위 명령을 포함합니다. 이러한 하위 명령을 사용하여 변경한 내용은 글로벌 구성 파일과 지시 파일에 기록됩니다. 셀 관리 도구를 사용하는 방법에 대한 정보는 [장 5 셀 관리 도구 참조 사항](#)의 내용을 참조하십시오.

사전 요구 사항

- 대화형 구성의 경우 [대화형 구성 참조](#) 항목을 검토합니다.
- 자동 구성의 경우 [자동 구성 참조](#) 항목을 검토합니다.
- 자동 구성의 경우 환경 변수 `VCLLOUD_HOME`의 값이 VMware Cloud Director가 설치되어 있는 디렉터리의 전체 경로 이름으로 설정되어 있는지 확인합니다. 이 값은 보통 `/opt/vmware/vcloud-director`입니다.

절차

1 VMware Cloud Director 서버에 루트로 로그인합니다.

2 `configure` 명령을 실행합니다.

- 대화형 모드의 경우 명령을 실행하고 프롬프트에서 필요한 정보를 입력합니다.

```
/opt/vmware/vcloud-director/bin/configure
```

- 자동 모드의 경우 적절한 옵션과 인수로 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/configure options -unattended
```

스크립트에서 정보가 확인되면 다음으로:

- a 데이터베이스가 초기화되고 서버가 여기에 연결됩니다.
- b VMware Cloud Director 서비스가 시작된 후 **VMware Cloud Director 설치** 마법사에 연결할 수 있는 URL이 표시됩니다.
- c VMware Cloud Director 셸 시작을 제안하는 메시지가 표시됩니다.

3 (선택 사항) VMware Cloud Director 설치 마법사 URL을 기록해 두고 **y**를 입력하여 VMware Cloud Director 서비스를 시작합니다.

나중에 `service vmware-vcd start` 명령을 실행하여 서비스를 시작하도록 결정할 수도 있습니다.

결과

구성 시 제공한 데이터베이스 연결 정보 및 기타 재사용 가능한 정보는 이 서버의 `/opt/vmware/vcloud-director/etc/responses.properties`에 있는 지시 파일에 보존됩니다. 이 파일에는 서버를 서버 그룹에 추가할 때 재사용해야 하는 중요한 정보가 포함되어 있습니다.

다음에 수행할 작업

안전한 위치에 지시 파일의 복사본을 저장합니다. 이 파일에 대한 액세스를 제한하고 안전한 위치에 백업 되도록 합니다. 파일을 백업하는 경우 공용 네트워크를 통해 일반 텍스트를 전송하지 마십시오.

서버 그룹에 서버를 추가하려는 경우 공유 전송 스토리지를 `/opt/vmware/vcloud-director/data/transfer`에 마운트합니다.

대화형 구성 참조

대화형 모드에서 `configure` 스크립트를 실행하는 경우 스크립트에 다음 정보를 묻는 메시지가 표시됩니다.

기본값을 그대로 적용하려면, Enter 키를 누릅니다.

표 4-1. 대화형 네트워크 및 데이터베이스 구성 중 필요한 정보

필요한 정보	설명
HTTPS 서비스의 IP 주소	기본값은 첫 번째로 사용 가능한 IP 주소입니다.
콘솔 프록시 서비스의 IP 주소	기본값은 첫 번째로 사용 가능한 IP 주소입니다. 참고 HTTPS 서비스 및 콘솔 프록시 서비스에 대해 서로 다른 두 개의 포트가 있는 단일 IP 주소를 사용하려는 경우에는 자동 모드에서 구성 스크립트를 실행해야 합니다.
Java 키 저장소 파일의 전체 경로	예를 들면 <code>/opt/keystore/certificates.ks</code> 와 같습니다.
키 저장소의 암호	Linux용 VMware Cloud Director 에 대한 SSL 인증서 를 만들기 전의 내용을 참조하십시오.

표 4-1. 대화형 네트워크 및 데이터베이스 구성 중 필요한 정보 (계속)

필요한 정보	설명
HTTPS SSL 인증서의 개인 키 암호	Linux용 VMware Cloud Director에 대한 SSL 인증서를 만들기 전의 내용을 참조하십시오.
콘솔 프록시 SSL 인증서의 개인 키 암호	Linux용 VMware Cloud Director에 대한 SSL 인증서를 만들기 전의 내용을 참조하십시오.
syslog 호스트에 대해 원격 감사 로깅을 사용하도록 설정	<p>각 VMware Cloud Director 셀의 서비스는 감사 메시지를 VMware Cloud Director 데이터베이스에 기록합니다. 감사 메시지는 여기서 90일 동안 보존됩니다. 감사 메시지를 더 길게 보존하기 위해 감사 메시지를 VMware Cloud Director 데이터베이스 외에 syslog 유틸리티에도 전송하도록 VMware Cloud Director 서비스를 구성할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 건너뛰려면 Enter 키를 누릅니다. ■ 사용하도록 설정하려면 syslog 호스트 이름 또는 IP 주소를 입력합니다.
원격 감사 로깅을 사용하도록 설정하는 경우, syslog 호스트의 UDP 포트	기본값은 514입니다.
데이터베이스 서버의 호스트 이름 또는 IP 주소	데이터베이스를 실행하는 서버.
데이터베이스 포트	기본값은 5432입니다.
데이터베이스 이름	기본값은 vcloud입니다.
데이터베이스 사용자 이름	Linux에서 VMware Cloud Director용 외부 PostgreSQL 데이터베이스 구성의 내용을 참조하십시오.
데이터베이스 암호	Linux에서 VMware Cloud Director용 외부 PostgreSQL 데이터베이스 구성의 내용을 참조하십시오.
VMware CEIP(고객 환경 향상 프로그램)에 참여 또는 참여 안 함	<p>이 제품은 VMware CEIP(고객 환경 향상 프로그램)에 참여합니다. CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 이러한 정보를 사용하는 목적은 Trust & Assurance Center(http://www.vmware.com/trustvmware/ceip.html)에 명시되어 있습니다. 셀 관리 도구를 사용하여 언제든지 이 제품에 대해 VMware의 CEIP에 참여하거나 탈퇴할 수 있습니다. 장 5 셀 관리 도구 참조 사항의 내용을 참조하십시오.</p> <p>프로그램에 참여하려면 y를 입력합니다.</p> <p>VMware의 CEIP 프로그램에 참여하지 않으려면 n을 입력합니다.</p>

자동 구성 참조

자동 모드에서 configure 스크립트를 실행하는 경우 명령줄에 설정 정보를 옵션 및 인수로 제공합니다.

표 4-2. 구성 유틸리티 옵션 및 인수

옵션	인수	설명
--help (-h)	없음	구성 옵션 및 인수의 요약을 표시합니다.
--config-file (-c)	global.properties 파일에 대한 경로	구성 유틸리티를 실행할 때 제공하는 정보가 이 파일에 저장됩니다. 이 옵션을 생략하면 기본 위치는 /opt/vmware/vcloud-director/etc/global.properties입니다.
--console-proxy-ip (-cons)	IPv4 주소, 선택적으로 포트 번호 포함 가능	시스템에서 VMware Cloud Director 콘솔 프록시 서비스에 대해 이 주소를 사용합니다. 예를 들어 10.17.118.159입니다.
--console-proxy-port-https	0-65535 사이의 정수	VMware Cloud Director 콘솔 프록시 서비스에 대해 사용할 포트 번호입니다.
--database-ssl	true 또는 false	VMware Cloud Director에서 잘 서명된 SSL 연결을 요구하도록 PostgreSQL 데이터베이스를 구성할 수 있습니다. 자체 서명된 인증서 또는 개인 인증서를 사용하도록 PostgreSQL 데이터베이스를 구성하려면 외부 PostgreSQL 데이터베이스에서 추가 구성 수행 항목을 참조하십시오.
--database-host (-dbhost)	VMware Cloud Director 데이터베이스 호스트의 IP 주소 또는 FQDN(정규화된 도메인 이름)	Linux에서 VMware Cloud Director 용 외부 PostgreSQL 데이터베이스 구성의 내용을 참조하십시오.
--database-name (-dbname)	데이터베이스 서비스 이름	Linux에서 VMware Cloud Director 용 외부 PostgreSQL 데이터베이스 구성의 내용을 참조하십시오.
--database-password (-dbpassword)	데이터베이스 사용자의 암호. null일 수 있습니다.	Linux에서 VMware Cloud Director 용 외부 PostgreSQL 데이터베이스 구성의 내용을 참조하십시오.
--database-port (-dbport)	데이터베이스 호스트의 데이터베이스 서비스에 서 사용하는 포트 번호	Linux에서 VMware Cloud Director 용 외부 PostgreSQL 데이터베이스 구성의 내용을 참조하십시오.
--database-type (-dbtype)	데이터베이스 유형. 지 원되는 유형은 postgres입니다.	선택 사항입니다. 데이터베이스 유형은 기본적으로 postgres입니다. Linux에서 VMware Cloud Director 용 외부 PostgreSQL 데이터베이스 구성의 내용을 참조하십시오.

표 4-2. 구성 유틸리티 옵션 및 인수 (계속)

옵션	인수	설명
--database-user (-dbuser)	데이터베이스 사용자의 사용자 이름.	Linux에서 VMware Cloud Director 용 외부 PostgreSQL 데이터베이스 구성의 내용을 참조하십시오.
--enable-ceip	true 또는 false	이 제품은 VMware CEIP(고객 환경 항상 프로그램)에 참여합니다. CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 이러한 정보를 사용하는 목적은 Trust & Assurance Center(http://www.vmware.com/trustvmware/ceip.html)에 명시되어 있습니다. 셀 관리 도구를 사용하여 언제든지 이 제품에 대해 VMware의 CEIP에 참여하거나 탈퇴할 수 있습니다. 장 5 셀 관리 도구 참조 사항 의 내용을 참조하십시오.
--uuid (-g)	없음	셀에 대한 새로운 고유 식별자를 생성합니다.
--primary-ip (-ip)	IPv4 주소, 선택적으로 포트 번호 포함 가능	시스템에서 VMware Cloud Director 웹 인터페이스 서비스에 대해 이 주소를 사용합니다. 예를 들어 10.17.118.159입니다.
--primary-port-http	0 ~ 65535 사이의 정수	VMware Cloud Director 웹 인터페이스 서비스에 대한 HTTP(비보안) 연결에 사용할 포트 번호
--primary-port-https	0-65535 사이의 정수	VMware Cloud Director 웹 인터페이스 서비스에 대한 HTTPS(보안) 연결에 사용할 포트 번호
--keystore (-k)	SSL 인증서와 개인 키가 들어 있는 Java keystore에 대한 경로	전체 경로 이름을 사용해야 합니다. 예를 들면 /opt/keystore/certificates.ks와 같습니다.
--syslog-host (-loghost)	syslog 서버 호스트의 IP 주소 또는 FQDN(정규화된 도메인 이름)	각 VMware Cloud Director 셀의 서비스는 감사 메시지를 VMware Cloud Director 데이터베이스에 기록합니다. 감사 메시지는 여기서 90일 동안 보존됩니다. 감사 메시지를 더 길게 보존하기 위해 감사 메시지를 VMware Cloud Director 데이터베이스 외에 syslog 유틸리티에도 전송하도록 VMware Cloud Director 서비스를 구성할 수 있습니다.

표 4-2. 구성 유틸리티 옵션 및 인수 (계속)

옵션	인수	설명
--syslog-port (-logport)	0-65535 사이의 정수	syslog 프로세스에서 지정된 서버를 모니터링하는 포트입니다. 지정하지 않는 경우 기본적으로 514로 설정됩니다.
--response-file (-r)	지시 파일에 대한 경로	전체 경로 이름을 사용해야 합니다. 지정하지 않는 경우 기본적으로 /opt/vmware/vcloud-director/etc/responses.properties로 설정됩니다. 구성을 실행할 때 제공하는 모든 정보가 이 파일에 보존됩니다. 중요 이 파일에는 서버를 서버 그룹에 추가할 때 재사용해야 하는 중요한 정보가 포함되어 있습니다. 필요시 사용할 수 있도록 파일을 안전한 장소에 보관하십시오.
--unattended-installation (-unattended)	없음	자동 설치를 지정합니다.
--keystore-password (-w)	SSL 인증서 keystore 암호	SSL 인증서 keystore 암호입니다.

예제: 두 개의 IP 주소로 자동 구성

다음은 HTTPS 서비스 및 콘솔 프록시 서비스에 대해 서로 다른 두 개의 IP 주소를 사용하여 VMware Cloud Director 서버의 자동 구성을 실행하는 명령의 예입니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype postgres -dbhost 10.150.10.78 -dbname postgresql-db-name -dbuser vcloud --enable-
ceip true \
-dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret -loghost 10.150.10.10
-unattended
```

예제: 단일 IP 주소로 자동 구성

다음은 HTTPS 서비스 및 콘솔 프록시 서비스에 대해 서로 다른 두 개의 포트가 있는 단일 IP 주소를 사용하여 VMware Cloud Director 서버의 자동 구성을 실행하는 명령의 예입니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./configure -ip 10.17.118.159 --primary-port-https 9000 -cons 10.17.118.159 \
--console-proxy-port-https 9010 -dbtype postgres -dbhost 10.150.10.78 -dbname postgresql-db-
name \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

지시 파일 보호 및 재사용

첫 번째 VMware Cloud Director 셀에서 구성하는 네트워크 및 데이터베이스 연결 세부 정보는 지시 파일에 저장됩니다. 이 파일에는 서버를 서버 그룹에 추가할 때 재사용해야 하는 중요한 정보가 포함되어 있습니다. 파일을 안전한 위치에 보존해야 합니다.

지시 파일은 네트워크 및 데이터베이스 연결을 구성하는 첫 번째 서버의 `/opt/vmware/vcloud-director/etc/responses.properties`에 만들어집니다. 그룹에 서버를 추가하는 경우에는 지시 파일의 사본을 사용하여 모든 서버가 공유하는 구성 매개 변수를 제공해야 합니다.

중요 셀 관리 도구는 처음에 지정한 네트워크 및 데이터베이스 연결 세부 정보를 변경하는 데 사용할 수 있는 하위 명령을 포함합니다. 이러한 도구로 수행된 변경 내용은 글로벌 구성 파일과 지시 파일에 기록되므로 파일을 변경할 수 있는 명령을 사용하기 전에 지시 파일이 제 위치(`/opt/vmware/vcloud-director/etc/responses.properties`)에 있는지 그리고 쓸 수 있는 상태인지 확인해야 합니다.

절차

1 지시 파일을 보호합니다.

안전한 위치에 파일의 사본을 저장합니다. 이 파일에 대한 액세스를 제한하고 안전한 위치에 백업되도록 합니다. 파일을 백업하는 경우 공용 네트워크를 통해 일반 텍스트를 전송하지 마십시오.

2 지시 파일을 다시 사용합니다.

a 구성할 준비가 된 서버가 액세스할 수 있는 위치에 파일을 복사합니다.

참고 지시 파일을 재사용하여 서버를 구성하려면 먼저 서버에 VMware Cloud Director 소프트웨어를 설치해야 합니다. 이 예제에 나온 대로 지시 파일의 경로 이름에 포함된 모든 디렉터리는 `vcloud.vcloud` 사용자가 읽을 수 있어야 합니다.

```
[root@cell11 /tmp]# ls -l responses.properties
-rw----- 1 vcloud vcloud 418 Jun 8 13:42 responses.properties
```

설치 관리자가 이 사용자 및 그룹을 만듭니다.

b `-r` 옵션을 사용하고 지시 파일 경로 이름을 지정하여 구성 스크립트를 실행합니다.

루트로 로그인하고, 콘솔, 셀 또는 터미널 창을 열고 다음을 입력합니다.

```
[root@cell11 /tmp]# /opt/vmware/vcloud-director/bin/configure -r /path-to-response-file
```

다음에 수행할 작업

추가 서버를 구성한 후에는 해당 서버를 구성하는 데 사용한 지시 파일의 사본을 삭제합니다.

서버 그룹의 추가 구성원에 VMware Cloud Director 설치

언제든지 VMware Cloud Director 서버 그룹에 서버를 추가할 수 있습니다. 서버 그룹에 속한 모든 서버는 동일한 데이터베이스 연결 정보를 사용하여 구성되어야 하므로 그룹의 첫 번째 구성원을 구성할 때 만든 지시 파일을 사용해야 합니다.

중요 하나의 서버 그룹에서 Linux에 설치된 VMware Cloud Director 및 VMware Cloud Director 장치 배포의 혼합은 지원되지 않습니다.

사전 요구 사항

- 이 서버 그룹의 첫 번째 구성원을 구성할 때 만들어진 지시 파일에 액세스할 수 있는지 확인합니다. [네트워크 및 데이터베이스 연결 구성](#)의 내용을 참조하십시오.
- VMware Cloud Director 서버 그룹의 첫 번째 구성원의 `/opt/vmware/vcloud-director/data/transfer`에 공유 전송 스토리지를 마운트했는지 확인합니다.

절차

- 1 대상 서버에 **root**로 로그인합니다.

- 2 설치 파일을 대상 서버에 다운로드합니다.

미디어에 있는 소프트웨어를 구입한 경우에는 대상 서버가 액세스할 수 있는 위치에 설치 파일을 복사하십시오.

- 3 설치 파일을 실행할 수 있는지 확인합니다.

설치 파일은 **실행** 권한이 있어야 실행할 수 있습니다. 이 권한이 있는지 확인하려면 콘솔, 셸 또는 터미널 창을 열고 다음 Linux 명령을 실행합니다. 명령에서 *installation-file*은 VMware Cloud Director 설치 파일의 전체 경로 이름입니다.

```
[root@cell11 /tmp]# chmod u+x installation-file
```

- 4 설치 파일을 실행합니다.

설치 파일을 실행하려면 다음과 같이 전체 경로 이름을 입력합니다.

```
[root@cell11 /tmp]# ./installation-file
```

이 파일에는 설치 스크립트와 내장된 RPM 패키지가 포함되어 있습니다.

참고 공백이 포함된 디렉터리가 해당 경로 이름에 있는 설치 파일은 실행할 수 없습니다.

대상 서버에 VMware 공용 키를 설치하지 않은 경우에는 설치 관리자에 다음과 같은 형식의 경고가 출력됩니다.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

설치 관리자는 다음 작업을 수행합니다.

- a 호스트가 모든 요구 사항을 충족하는지 확인합니다.
- b 설치 파일의 디지털 서명을 확인합니다.
- c vcloud 사용자 및 그룹을 만듭니다.
- d VMware Cloud Director RPM 패키지의 압축을 풉니다.
- e 소프트웨어를 설치합니다.

설치가 끝나면, 네트워크 및 데이터베이스 연결을 구성하는 구성 스크립트를 실행하라는 메시지가 설치 관리자에 표시됩니다.

- 5 **n**을 입력하고 **Enter** 키를 눌러서 구성 스크립트 실행을 거부합니다.

나중에 지시 파일을 입력으로 제공하여 구성 스크립트를 실행합니다.

- 6 공유 전송 스토리지를 /opt/vmware/vcloud-director/data/transfer에 마운트합니다.

서버 그룹의 모든 VMware Cloud Director 서버는 동일한 마운트 지점에 이 볼륨을 마운트해야 합니다.

- 7 이 서버가 액세스할 수 있는 위치에 지시 파일을 복사합니다.

지시 파일의 경로 이름에 포함된 모든 디렉터리를 루트가 읽을 수 있어야 합니다.

- 8 구성 스크립트를 실행합니다.

- a 지시 파일 경로 이름을 제공하여 configure 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/configure -r /responses.properties
```

스크립트는 vcloud.vcloud에서 읽을 수 있는 위치에 지시 파일을 복사하고 지시 파일을 입력으로 사용하여 구성 스크립트를 실행합니다.

- b 프롬프트에 HTTP 및 콘솔 프록시 서비스에 대한 IP 주소를 입력합니다.

- c 구성 스크립트가 지시 파일에 저장된 경로 이름에서 유효한 인증서를 찾지 못하는 경우에는 프롬프트가 표시되면 인증서의 경로 이름과 암호를 제공합니다.

스크립트가 정보를 확인하고 서버를 데이터베이스에 연결하고 VMware Cloud Director 셀을 시작하도록 제안합니다.

- 9 (선택 사항) **y**를 입력하여 VMware Cloud Director 서비스를 시작합니다.

나중에 `service vmware-vcd start` 명령을 실행하여 서비스를 시작하도록 결정할 수도 있습니다.

다음에 수행할 작업

서버 그룹에 서버를 더 추가하려면 이 절차를 반복합니다.

모든 서버에서 VMware Cloud Director 서비스가 실행되면 라이선스 키, 시스템 관리자 계정 및 관련 정보를 사용하여 VMware Cloud Director 데이터베이스를 초기화해야 합니다. `system-setup` 하위 명령과 함께 셸 관리 도구를 사용하여 데이터베이스를 초기화할 수 있습니다. [VMware Cloud Director 설치 구성](#)의 내용을 참조하십시오.

VMware Cloud Director 설치 후 작업

VMware Cloud Director 서버 그룹을 생성한 후에는 Microsoft Sysprep 파일 및 Cassandra 데이터베이스를 설치할 수 있습니다. PostgreSQL 데이터베이스를 사용하는 경우에는 데이터베이스에서 SSL을 구성하고 일부 매개 변수를 조정할 수 있습니다.

버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)의 내용을 참조하십시오.

Linux용 VMware Cloud Director에 대한 공개 주소 사용자 지정

로드 밸런서 또는 프록시 요구 사항을 충족하기 위해 VMware Cloud Director 웹 포털, VMware Cloud Director API 및 콘솔 프록시에 대한 기본 끝점 웹 주소를 변경할 수 있습니다.

사전 요구 사항

시스템 관리자로 로그인했는지 확인합니다. **시스템 관리자**만 공용 끝점을 사용자 지정할 수 있습니다.

절차

- 1 Service Provider Admin Portal의 위쪽 탐색 모음에서 **관리**를 선택합니다.
- 2 왼쪽 창의 **설정** 아래에서 **공개 주소**를 클릭합니다.
- 3 공용 끝점을 사용자 지정하려면 **편집**을 클릭합니다.
- 4 VMware Cloud Director URL을 사용자 지정하려면 **웹 포털** 끝점을 편집합니다.
 - a HTTP(비보안) 연결을 위한 사용자 지정 VMware Cloud Director 공용 URL을 입력합니다.
 - b HTTPS(보안) 연결을 위한 사용자 지정 VMware Cloud Director 공용 URL을 입력하고 **업로드**를 클릭하여 해당 끝점의 신뢰 체인을 설정하는 인증서를 업로드합니다.

인증서 체인은 서비스 끝점에서 사용되는 인증서와 일치해야 하며, 이것은 별칭이 `consoleproxy` 인 각 VMware Cloud Director 셸 키 저장소에 업로드된 인증서입니다. 로드 밸런서에서 콘솔 프록시 연결의 SSL 종료는 지원되지 않습니다. 인증서 체인에는 끝점 인증서, 중간 인증서 및 개인 키 없는 PEM 형식의 루트 인증서가 포함되어야 합니다.

- 5 (선택 사항) Cloud Director REST API와 OpenAPI URL을 사용자 지정하려면 **웹 포털 설정 사용** 토글을 해제합니다.

- a 사용자 지정 HTTP 기본 URL을 입력합니다.

예를 들어 HTTP 기본 URL을 **http://vcloud.example.com**으로 설정하면 http://vcloud.example.com/api에서 VMware Cloud Director API에 액세스하고 http://vcloud.example.com/cloudapi에서 VMware Cloud Director OpenAPI에 액세스할 수 있습니다.

- b 사용자 지정 HTTPS REST API 기본 URL을 입력하고 **업로드**를 클릭하여 해당 끝점의 신뢰 체인을 설정하는 인증서를 업로드합니다.

예를 들어 HTTPS REST API 기본 URL을 **https://vcloud.example.com**으로 설정하면 https://vcloud.example.com/api에서 VMware Cloud Director API에 액세스하고 https://vcloud.example.com/cloudapi에서 VMware Cloud Director OpenAPI에 액세스할 수 있습니다.

인증서 체인은 서비스 끝점에 사용되는 인증서와 일치해야 하며, 별칭이 http인 각 VMware Cloud Director 셀 키 저장소에 업로드된 인증서이거나 SSL 종료가 사용되는 경우 로드 밸런서 VIP 인증서입니다. 인증서 체인에는 끝점 인증서, 중간 인증서 및 개인 키 없는 PEM 형식의 루트 인증서가 포함되어야 합니다.

- 6 사용자 지정 VMware Cloud Director 공용 콘솔 프록시 주소를 입력합니다.

이 주소는 포트 번호가 있는 로드 밸런서 또는 VMware Cloud Director 서버의 FQDN(정규화된 도메인 이름)입니다. 기본 포트는 443입니다.

중요 VMware Cloud Director 장치는 콘솔 프록시 서비스에 대해 사용자 지정 포트가 8443인 자체 eth0 NIC를 사용합니다.

예를 들어 FQDN이 vcloud.example.com인 VMware Cloud Director 장치 인스턴스의 경우 **vcloud.example.com:8443**을 입력합니다.

VMware Cloud Director는 VM에서 원격 콘솔 창을 열 때 콘솔 프록시 주소를 사용합니다.

- 7 변경 내용을 저장하려면 **저장**을 클릭합니다.

기간별 메트릭 데이터 저장을 위한 Cassandra 데이터베이스 설치 및 구성

VMware Cloud Director는 클라우드에 있는 가상 시스템의 가상 시스템 성능 및 리소스 사용에 대한 현재 및 이전 정보를 제공하는 메트릭을 수집할 수 있습니다. 이전 메트릭에 대한 데이터는 Cassandra 클러스터에 저장됩니다.

Cassandra는 오픈 소스 데이터베이스로, 가상 시스템 메트릭과 같은 시계열 데이터를 수집하는 확장 가능한 고성능 솔루션용 백업 저장소를 제공하는 데 사용할 수 있습니다. VMware Cloud Director에서 가상 시스템의 이전 메트릭 검색을 지원하도록 하려면 Cassandra 클러스터를 설치 및 구성하고 cell-management-tool을 사용하여 클러스터를 VMware Cloud Director에 연결해야 합니다. 현재 메트릭을 검색할 경우에는 데이터베이스 소프트웨어(선택 사항)가 필요하지 않습니다.

사전 요구 사항

- 데이터베이스 소프트웨어(선택 사항)를 구성하기 전에 VMware Cloud Director가 설치되어 실행 중인지 확인합니다.
- Cassandra에 아직 익숙하지 않은 경우 <http://cassandra.apache.org/>에서 자료를 검토합니다.
- 메트릭 데이터베이스로 사용하기 위해 지원되는 Cassandra 릴리스 목록은 "VMware Cloud Director 릴리스 정보" 항목을 참조하십시오. <http://cassandra.apache.org/download/>에서 Cassandra를 다운로드할 수 있습니다.
- Cassandra 클러스터 설치 및 구성:
 - Cassandra 클러스터에는 2개 이상의 호스트에 배포된 4개 이상의 가상 시스템이 포함되어야 합니다.
 - 2개의 Cassandra 시드 노드가 필요합니다.
 - Cassandra 클라이언트와 노드 간 암호화를 사용하도록 설정합니다. <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html>의 내용을 참조하십시오.
 - Cassandra 사용자 인증을 사용하도록 설정합니다. <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html>의 내용을 참조하십시오.
 - 각 Cassandra 클러스터에서 JNA(Java Native Access) 버전 3.2.7 이상을 사용하도록 설정합니다.
 - Cassandra 노드 간 암호화는 선택 사항입니다.
 - Cassandra에서 SSL의 사용은 선택 사항입니다. Cassandra에 대한 SSL을 사용하도록 설정하지 않는 경우 각 셀(\$VCLLOUD_HOME/etc/global.properties)의 global.properties 파일에서 구성 매개 변수 `cassandra.use.ssl`을 0으로 설정해야 합니다.

절차

- 1 cell-management-tool 유틸리티를 사용하여 VMware Cloud Director와 Cassandra 클러스터의 노드 간에 연결을 구성합니다.

다음 명령 예에서 *node1-ip*, *node2-ip*, *node3-ip* 및 *node4-ip*는 Cassandra 클러스터 구성원의 IP 주소입니다. 기본 포트(9042)가 사용됩니다. 메트릭 데이터는 15일 동안 유지됩니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
```

셀 관리 도구를 사용하는 방법에 대한 정보는 [장 5 셀 관리 도구 참조 사항](#)의 내용을 참조하십시오.

- 2 (선택 사항) VMware Cloud Director를 버전 9.1에서 업그레이드하는 경우 `cell-management-tool`을 사용하여 메트릭 데이터베이스가 롤업된 메트릭을 저장하도록 구성합니다.

다음 예와 유사한 명령을 실행합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password
'P@55w0rd'
```

- 3 각 VMware Cloud Director 셀을 다시 시작합니다.

외부 PostgreSQL 데이터베이스에서 추가 구성 수행

VMware Cloud Director 서버 그룹을 만든 후에는 VMware Cloud Director 셀에서 SSL 연결을 요구하도록 외부 PostgreSQL 데이터베이스를 구성하고 최적의 성능을 위해 일부 데이터베이스 매개 변수를 조정할 수 있습니다.

가장 안전한 연결을 위해서는 잘 서명된 SSL 인증서가 필요합니다. 여기에는 잘 알려진 공인 인증 기관을 기반으로 하는 완전한 신뢰 체인이 포함됩니다. 또는 자체 서명된 SSL 인증서나 사설 인증 기관에서 서명한 SSL 인증서를 사용할 수 있지만 해당 인증서를 VMware Cloud Director truststore로 가져와야 합니다.

시스템 사양 및 요구 사항에 맞는 최적의 성능을 확보하려면, 데이터베이스 구성 파일에서 `autovacuum` 매개 변수 및 데이터베이스 구성을 조정할 수 있습니다.

절차

- 1 VMware Cloud Director와 PostgreSQL 데이터베이스 사이에 SSL 연결을 구성합니다.

- a 외부 PostgreSQL 데이터베이스에 대해 자체 서명된 인증서나 개인 인증서를 사용하는 경우, 각 VMware Cloud Director 셀에서 다음 명령을 실행하여 VMware Cloud Director truststore로 데이터베이스 인증서를 가져옵니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool import-trusted-certificates --source path_to_self-
signed_or_private_cert
```

- b 다음 명령을 실행하여 VMware Cloud Director와 PostgreSQL 사이에 SSL 연결을 사용하도록 설정합니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]#
cell-management-tool reconfigure-database --database-ssl true
```

--private-key-path 옵션을 사용하면 서버 그룹의 모든 셀에 대해 명령을 실행할 수 있습니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]#
cell-management-tool reconfigure-database --database-ssl true --private-key-
path path_to_private_key
```

셀 관리 도구를 사용하는 방법에 대한 자세한 내용은 [장 5 셀 관리 도구 참조 사항](#)의 내용을 참조하십시오.

- 2 현재 시스템 규격에 맞게 `postgresql.conf` 파일에서 데이터베이스 구성을 편집합니다.

예를 들어, 메모리가 16GB인 시스템의 경우 다음 부분을 사용할 수 있습니다.

```
max_connections = 500
# Set effective cache size to 50% of total memory.
effective_cache_size = 8GB
# Set shared buffers to 25% of total memory
shared_buffers = 4GB
```

- 3 요구 사항에 맞게 `postgresql.conf` 파일의 `autovacuum` 매개 변수를 편집합니다.

일반적인 VMware Cloud Director 워크로드의 경우 다음 부분을 사용할 수 있습니다.

```
autovacuum = on
track_counts = on
autovacuum_max_workers = 3
autovacuum_naptime = 1min
autovacuum_vacuum_cost_limit = 2400
```

시스템에서 활동 및 `activity_parameters` 테이블에 대한 사용자 지정 `autovacuum_vacuum_scale_factor` 값이 설정됩니다.

다음에 수행할 작업

`postgresql.conf` 파일을 편집한 경우에는 데이터베이스를 다시 시작해야 합니다.

RabbitMQ AMQP 브로커 설치 및 구성

차단 작업, 알림 또는 VMware Cloud Director API 확장(예: Container Service Extension (CSE) 또는 VMware Cloud Director App Launchpad)을 사용하려면 RabbitMQ AMQP 브로커를 설치하고 구성해야 합니다.

AMQP(Advanced Message Queuing Protocol)는 기업 시스템에 유연한 메시징을 지원하는 메시지 대기열 기능의 개방형 표준입니다. VMware Cloud Director는 확장 서비스, 개체 확장 및 알림에 사용되는 메시지 버스를 제공하기 위해 RabbitMQ AMQP 브로커를 사용합니다.

VMware Cloud Director의 경우, 알림을 구성할 때 RabbitMQ AMQP 브로커 대신 MQTT 클라이언트를 사용할 수 있습니다. [MQTT 클라이언트를 사용하여 이벤트, 작업 및 메트릭 구독의 내용을 참조하십시오.](#)

절차

- 1 <https://www.rabbitmq.com/download.html>에서 RabbitMQ Server를 다운로드합니다.

지원되는 RabbitMQ 릴리스의 목록을 보려면 "VMware Cloud Director 릴리스 정보"를 참조하십시오.

2 RabbitMQ 설치 지침에 따라 RabbitMQ를 지원되는 호스트에 설치합니다.

각 VMware Cloud Director 셀에서 네트워크에 있는 RabbitMQ 서버 호스트에 액세스할 수 있어야 합니다.

3 RabbitMQ를 설치하는 동안 이 RabbitMQ 설치 환경과 연동하도록 VMware Cloud Director를 구성하는 데 필요한 값을 기록해 둡니다.

- RabbitMQ 서버 호스트의 정규화된 도메인 이름(예: *amqp.example.com*)
- RabbitMQ를 인증하는 데 유효한 사용자 이름과 암호
- 브로커가 메시지를 수신하는 포트입니다. 기본값은 비SSL의 경우 5672입니다. SSL/TLS에 대한 기본 포트는 5671입니다.
- 통신 프로토콜은 TCP입니다.
- RabbitMQ 가상 호스트입니다. 기본값은 "/"입니다.

다음에 수행할 작업

기본적으로 VMware Cloud Director AMQP 서비스는 암호화되지 않은 메시지를 보냅니다. SSL을 사용하여 이러한 메시지를 암호화하도록 AMQP 서비스를 구성할 수 있습니다. VMware Cloud Director 셀에 있는(일반적인 위치: `$VCLLOUD_HOME/jre/lib/security/cacerts`) Java Runtime Environment의 기본 JCEKS 신뢰 저장소를 사용하여 브로커 인증서를 확인하도록 서비스를 구성할 수도 있습니다.

VMware Cloud Director AMQP 서비스에서 SSL을 사용하도록 설정하려면 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 [AMQP 브로커 구성](#) 정보를 참조하십시오.

MQTT 클라이언트를 사용하여 이벤트, 작업 및 메트릭 구독

MQTT 클라이언트를 사용하여 VMware Cloud Director 이벤트 및 작업에 대한 메시지를 구독할 수 있습니다.

MQTT는 경량, 바이너리, 메시징 전송 프로토콜입니다. VMware Cloud Director는 MQTT를 사용하여 이벤트 및 작업에 대한 정보를 게시하며, 사용자는 MQTT 클라이언트를 사용하여 메시지를 구독할 수 있습니다. MQTT 메시지는 MQTT 브로커를 통과하며, 이 브로커는 클라이언트가 온라인 상태가 아닌 경우에도 메시지를 저장할 수 있습니다.

VMware Cloud Director 10.2.2부터는 MQTT 클라이언트를 사용하여 메트릭을 구독할 수 있습니다.

사전 요구 사항

- WebSocket을 지원하는 MQTT 클라이언트가 있는지 확인합니다.
- WebSocket 업그레이드된 요청에 헤더를 추가할 수 있는지 확인합니다.
- 메트릭을 구독하려면 메트릭 수집을 구성하고 메트릭 게시를 사용하도록 설정합니다. [메트릭 수집 및 게시 구성](#)의 내용을 참조하십시오.

절차

1 OpenAPI 끝점을 사용하여 VMware Cloud Director에 로그인합니다.

- 2 WebSocket 연결을 설정하려면 **Sec-WebSocket-Protocol** 속성을 `mqt`로 설정하고, 클라이언트를 `/messaging/mqt` 경로에 연결하도록 설정하고, 인증 헤더를 추가하고, 표준 **MQTT** 연결 흐름을 따릅니다.

VMware Cloud Director에 대한 표준 로그인 요청에서 **JWT** 토큰을 수신합니다. 사용자 이름과 암호는 비워 둘 수 있습니다.

```
Sec-WebSocket-Protocol: mqt
```

```
Authorization: Bearer {JWT_token}
```

- 3 연결이 성공적으로 설정되면 **MQTT** 클라이언트를 통해 항목을 구독합니다.

```
publish/{user_org_id}/{user_id}
```

```
publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
```

조직 관리자는 와일드카드를 사용하여 모든 조직 항목에 액세스할 수 있습니다.

```
publish/{user_org_id}/+
```

시스템 관리자는 와일드카드를 사용하여 모든 항목에 액세스할 수 있습니다.

```
publish/#
```

- 4 (선택 사항) VMware Cloud Director 10.2.2 이상인 경우 메트릭을 구독합니다.

```
metrics/{org_id}/{vApp_id}
```

시스템 관리자만 메트릭 항목에 액세스할 수 있습니다.

자동 스케일 그룹

VMware Cloud Director 10.2.2부터는 현재 **CPU** 및 메모리 사용에 따라 테넌트 사용자가 애플리케이션을 자동 스케일링하도록 허용할 수 있습니다.

CPU 및 메모리 사용에 대해 미리 정의한 조건에 따라, 테넌트는 **VMware Cloud Director**를 사용하여 선택한 스케일 그룹의 **VM** 수를 자동으로 스케일 업/다운할 수 있습니다. 테넌트가 애플리케이션을 자동으로 스케일링하도록 허용하려면 자동 스케일 솔루션에 대한 액세스 권한을 구성, 게시 및 부여해야 합니다.

동일한 애플리케이션을 실행하도록 구성된 서버에 대해 로드 밸런싱을 수행하려면 **VMware NSX Advanced Load Balancer(Avi Networks)**를 사용하면 됩니다.

자동 스케일 플러그인 구성 및 게시

테넌트에 대한 액세스 권한을 부여하기 전에 자동 스케일 그룹 솔루션을 구성해야 합니다. 자동 스케일링은 **VMware Cloud Director 10.2.2**부터 사용할 수 있습니다.

- 1 클러스터에 있는 셀의 **OS**에 **root**로 직접 로그인하거나 **SSH** 클라이언트를 사용하여 로그인합니다.

- 2 Cassandra 데이터베이스에서 메트릭 수집을 설정하여 메트릭 데이터 수집을 사용하도록 설정하거나 메트릭 데이터 지속성 없이 메트릭을 수집합니다.

- 기간별 메트릭 데이터 저장을 위한 **Cassandra** 데이터베이스 설치 및 구성
- 데이터 지속성 없이 메트릭 데이터를 수집하려면 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.collect.only -v true
```

- 3 메트릭 게시를 사용하도록 설정합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

- 4 /tmp 폴더에 다음 내용으로 metrics.groovy 파일을 생성합니다.

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
        instance=""
        minReportingInterval=300
        aggregator="AVERAGE"
    }
}
```

- 5 파일을 가져옵니다.

```
$VCLLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
metrics.groovy
```

- 6 이전에 **Cassandra**를 구성한 경우 올바른 노드 주소, 데이터베이스 인증 세부 정보, 포트 및 메트릭 TTL(Time to Live)(일)을 제공하여 **Cassandra** 스키마를 업데이트합니다.

```
$VCLLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -
ttl TTL_days -update-schema
```

- 7 CA 서명된 인증서를 사용하여 셀을 실행하는 경우 자동 스케일링을 사용하도록 설정하려면 다음 명령을 실행합니다.

```
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<username>
$VCLLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>
```

터미널에서 명령을 실행할 때 백슬래시(\) 기호를 사용하여 특수 문자를 이스케이프하십시오.

8 셀을 다시 시작합니다.

```
service vmware-vcd restart
```

9 자동 스케일 권한 번들 게시

자동 스케일 권한 번들 게시

테넌트가 애플리케이션을 자동 스케일링하도록 하려면 시스템에 있는 하나 이상의 조직에 권한 번들을 게시해야 합니다. 자동 스케일링은 VMware Cloud Director 10.2.2부터 사용할 수 있습니다.

사전 요구 사항

자동 스케일 플러그인 구성 및 게시

절차

- 1 위쪽 탐색 모음에서 **관리**를 선택합니다.
- 2 왼쪽 패널의 **테넌트 액세스 제어** 아래에서 **권한 번들**을 선택합니다.
- 3 자동 스케일링에 대한 액세스 권한을 부여하려는 테넌트 조직에 **레거시 권한 번들**이 없는지 확인합니다.
- 4 **vmware:scalegroup 사용 권한** 번들을 선택하고 **게시**를 클릭합니다.
- 5 번들을 게시하려면 다음을 수행합니다.
 - a **테넌트에 게시**를 선택합니다.
 - b 역할을 게시할 대상 조직을 선택합니다.
 - 시스템에 있는 기존 조직 및 새로 만든 조직 모두에 번들을 게시하려면 **모든 테넌트에 게시**를 선택합니다.
 - 시스템에 있는 특정 조직에 번들을 게시하려면 조직을 개별적으로 선택합니다.
- 6 **저장**을 클릭합니다.

다음에 수행할 작업

스케일 그룹을 사용하려는 테넌트 역할에 필요한 **VMWARE:SCALEGROUP** 권한을 추가합니다. 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"의 **글로벌 테넌트 역할 보기 및 편집**을 참조하십시오.

Linux에서 VMware Cloud Director 업그레이드

VMware Cloud Director를 새 버전으로 업그레이드하려면 서버 그룹의 모든 셀에서 VMware Cloud Director 서비스를 종료하고 각 서버에 새 버전을 설치하고 VMware Cloud Director 데이터베이스를 업그레이드한 다음 VMware Cloud Director 셀을 다시 시작합니다.

기존 VMware Cloud Director 서버 그룹이 Linux에 설치된 VMware Cloud Director로 구성된 경우 Linux용 VMware Cloud Director 설치 관리자를 사용하여 환경을 업그레이드할 수 있습니다.

Linux에 VMware Cloud Director를 설치할 경우 오케스트레이션된 업그레이드를 수행하거나 VMware Cloud Director를 수동으로 업그레이드할 수 있습니다. 자세한 내용은 [VMware Cloud Director 설치의 오케스트레이션된 업그레이드를 수행](#) 또는 [수동으로 VMware Cloud Director 설치를 업그레이드에 나와](#) 있습니다. 오케스트레이션된 업그레이드에서는 단일 명령을 실행하여 서버 그룹 및 데이터베이스의 모든 셀을 업그레이드합니다. 수동 업그레이드에서는 각 셀 및 데이터베이스를 차례로 업그레이드합니다.

VMware Cloud Director 9.5부터:

- Oracle 데이터베이스가 지원되지 않습니다. 기존 VMware Cloud Director 설치에서 Oracle 데이터베이스를 사용하는 경우 [업그레이드 경로 및 워크플로](#) 테이블을 참조하십시오.
- ESXi 호스트 활성화 및 비활성화는 지원되지 않습니다. 업그레이드를 시작하기 전에 모든 ESXi 호스트를 활성화해야 합니다. vSphere Client를 사용하여 ESXi 호스트를 유지 보수 모드로 전환할 수 있습니다.
- VMware Cloud Director는 향상된 LDAP 지원이 포함된 Java를 사용합니다. LDAPS 서버를 사용하는 경우 LDAP 로그인 실패를 방지하기 위해서 적절히 구성된 인증서가 있는지 확인해야 합니다. 자세한 내용은 <https://www.java.com>에서 "Java 8 릴리스 변경사항"을 참조하십시오.

VMware Cloud Director 10.0부터 Microsoft SQL Server 데이터베이스가 지원되지 않습니다.

VMware Cloud Director를 업그레이드 하는 경우 새 버전이 기존 설치의 다음 구성 요소와 호환되어야 합니다.

- VMware Cloud Director 데이터베이스에 현재 사용 중인 데이터베이스 소프트웨어. 자세한 내용은 [업그레이드 및 마이그레이션 경로](#) 테이블을 참조하십시오.
- 현재 사용 중인 VMware vSphere® 릴리스입니다.
- 현재 사용 중인 VMware NSX® 릴리스입니다.
- VMware Cloud Director와 직접 상호 작용하는 모든 타사 구성 요소.

VMware Cloud Director와 다른 VMware 제품 및 타사 데이터베이스와의 호환성에 대한 정보는 http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php에서 "VMware 제품 상호 운용성 매트릭스"를 참조하십시오. VMware Cloud Director 업그레이드의 일환으로 vSphere 또는 NSX 구성 요소를 업그레이드하려면 VMware Cloud Director를 업그레이드한 후에 업그레이드해야 합니다. [VMware Cloud Director 업그레이드 후 작업](#)의 내용을 참조하십시오.

하나 이상의 VMware Cloud Director 서버를 업그레이드한 후에 VMware Cloud Director 데이터베이스를 업그레이드할 수 있습니다. 데이터베이스는 실행 중인 모든 VMware Cloud Director 작업의 상태를 비롯한 서버의 런타임 상태에 대한 정보를 저장합니다. 업그레이드 후 잘못된 작업 정보가 데이터베이스에 남아 있지 않도록 하려면 업그레이드를 시작하기 전에 모든 서버에서 활성 상태의 작업이 없는지 확인해야 합니다.

또한 VMware Cloud Director 데이터베이스에 저장되지 않은 다음의 아티팩트도 업그레이드할 때 유지됩니다.

- 로컬 및 전역 속성 파일은 새 설치 환경에 복사됩니다.
- 게스트 사용자 지정 지원에 사용되는 Microsoft Sysprep 파일은 새 설치 환경에 복사됩니다.

이 업그레이드에는 서버 그룹 및 데이터베이스의 모든 서버를 업그레이드하기에 충분한 VMware Cloud Director 다운타임이 필요합니다. 로드 밸런서를 사용하는 경우 메시지(예: 시스템이 업그레이드를 위해 오프라인 상태입니다.)를 반환하도록 로드 밸런서를 구성할 수 있습니다.

버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. [테스트 연결 거부 목록 구성](#)의 내용을 참조하십시오.

중요 버전 10.1 이상으로 업그레이드한 후 VMware Cloud Director는 연결된 모든 인프라 끝점에 대한 인증서를 항상 확인합니다. 이는 VMware Cloud Director가 SSL 인증서를 관리하는 방식이 변경되었기 때문입니다. 업그레이드 전에 인증서를 VMware Cloud Director로 가져오지 않으면 SSL 확인 문제로 인해 vCenter Server 및 NSX 연결에 실패한 연결 오류가 표시될 수 있습니다. 이 경우 업그레이드 후 다음 두 가지 옵션이 제공됩니다.

- 1 셸 관리 도구 trust-infra-certs 명령을 실행하여 모든 인증서를 중앙 집중식 인증서 저장소로 자동으로 가져옵니다. [vSphere 리소스에서 끝점 인증서 가져오기](#)를 참조하십시오.
- 2 Service Provider Admin Portal UI에서 각 vCenter Server 및 NSX 인스턴스를 선택하고 인증서를 수락하는 동안 자격 증명을 다시 입력합니다.

업그레이드 경로 및 워크플로

소스 환경	대상 환경	
	외부 PostgreSQL 데이터베이스를 사용하는 Linux의 VMware Cloud Director 10.2	
외부 Microsoft SQL Server 데이터베이스를 사용하는 Linux의 VMware Cloud Director 9.7	1	Microsoft SQL Server 데이터베이스를 PostgreSQL 데이터베이스로 마이그레이션합니다. PostgreSQL 데이터베이스로 마이그레이션 을 참조하십시오.
	2	환경을 Linux의 VMware Cloud Director 10.2로 업그레이드합니다. 자세한 내용은 VMware Cloud Director 설치의 오케스트레이션된 업그레이드 를 수행 또는 수동으로 VMware Cloud Director 설치를 업그레이드에 나와 있습니다 .
외부 PostgreSQL 데이터베이스를 사용하는 Linux의 VMware Cloud Director 9.7, 10.0 또는 10.1	환경을 Linux의 VMware Cloud Director 10.2로 업그레이드합니다. 자세한 내용은 VMware Cloud Director 설치의 오케스트레이션된 업그레이드 를 수행 또는 수동으로 VMware Cloud Director 설치를 업그레이드에 나와 있습니다 .	
내장형 PostgreSQL 데이터베이스를 사용하는 VMware Cloud Director 장치 9.7, 10.0 또는 10.1	지원되지 않음	

VMware Cloud Director 설치의 오케스트레이션된 업그레이드를 수행

--private-key-path 옵션으로 VMware Cloud Director 설치 관리자를 실행하면 공유 데이터베이스와 함께 서버 그룹의 모든 셀을 업그레이드 할 수 있습니다.

지원되는 Linux OS에서 Linux용 VMware Cloud Director 설치 관리자를 사용하여 VMware Cloud Director 설치로 구성된 VMware Cloud Director 서버 그룹을 업그레이드할 수 있습니다. VMware Cloud Director 서버 그룹이 VMware Cloud Director 9.5 장치 배포로 구성된 경우, Linux용 VMware Cloud Director 설치 관리자를 사용하여 마이그레이션 워크플로의 일부로만 기존 환경을 업그레이드합니다. [VMware Cloud Director 장치 업그레이드 및 마이그레이션](#)의 내용을 참조하십시오.

Linux용 VMware Cloud Director는 vmware-vcloud-director-distribution-v.v.v-"nnnnnn".bin 형식의 이름을 가지는 디지털 서명된 실행 파일로 배포됩니다. 여기서 v.v.v는 제품 버전을 나타내고 "nnnnnn"은 빌드 번호를 나타냅니다. 예를 들면 vmware-vcloud-director-distribution-8.10.0-3698331.bin과 같습니다. 이 실행 파일을 실행하면 VMware Cloud Director가 설치 또는 업그레이드됩니다.

--private-key-path 옵션과 함께 VMware Cloud Director 설치 관리자를 실행하는 경우 upgrade 유틸리티의 다른 명령 옵션(예: --maintenance-cell)을 추가할 수 있습니다. 데이터베이스 upgrade 유틸리티 옵션에 대한 자세한 내용은 [데이터베이스 업그레이드 유틸리티](#) 참조 항목을 참조하십시오.

사전 요구 사항

- VMware Cloud Director 데이터베이스, vSphere 구성 요소 및 NSX 구성 요소가 VMware Cloud Director의 새 버전과 호환되는지 확인합니다.

중요 기존 VMware Cloud Director 설치에서 Oracle 데이터베이스 또는 Microsoft SQL Server 데이터베이스를 사용하는 경우 업그레이드 전에 PostgreSQL 데이터베이스로 마이그레이션했는지 확인합니다. 가능한 업그레이드 경로는 [Linux에서 VMware Cloud Director 업그레이드](#)의 내용을 참조하십시오.

- 대상 서버에 대한 슈퍼 사용자 자격 증명이 있는지 확인합니다.
- 설치 관리자에서 설치 파일의 디지털 서명을 확인하려면 대상 서버에 VMware 공용 키를 다운로드하여 설치합니다. 설치 파일의 디지털 서명을 이미 확인한 경우 설치 중에 다시 확인할 필요가 없습니다. [VMware 공용 키 다운로드 및 설치](#)의 내용을 참조하십시오.
- 업그레이드할 버전의 VMware Cloud Director 소프트웨어를 사용할 수 있는 유효한 라이선스 키가 있는지 확인합니다.
- 모든 셀이 슈퍼유저의 SSH 연결을 암호 없이 허용하는지 확인합니다. 확인을 수행하려면 다음 Linux 명령을 실행하면 됩니다.

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

이 예제에서는 ID를 vcloud로 설정한 다음 *cell-ip*에 있는 셀에 루트로 SSH 연결을 설정하지만 루트 암호는 제공하지 않습니다. 로컬 셀의 *private-key-path*에 있는 개인 키를 vcloud.vcloud 사용자가 읽을 수 있고, 해당하는 공용 키가 *cell-ip*에서 루트 사용자의 *authorized-keys*에 있으면 명령이 성공합니다.

참고 VMware Cloud Director 프로세스가 실행되는 ID로 사용할 vcloud 사용자, vcloud 그룹 및 vcloud.vcloud 계정이 VMware Cloud Director 설치 관리자에 의해 생성됩니다. vcloud 사용자는 암호가 없습니다.

- 모든 ESXi 호스트가 활성화되었는지 확인합니다. 비활성화된 ESXi 호스트는 지원되지 않습니다.
- 서버 그룹의 모든 서버가 공유 전송 서버 스토리지에 액세스할 수 있는지 확인합니다. [Linux에서 VMware Cloud Director를 위한 전송 서버 스토리지 준비](#)의 내용을 참조하십시오.
- VMware Cloud Director 설치에 LDAPS 서버를 사용하는 경우에는 업그레이드 후 LDAP 로그인 실패를 방지하기 위해서 Java 8 Update 181에 맞게 적절히 구성된 인증서가 있는지 확인합니다. 자세한 내용은 <https://www.java.com>에서 "Java 8 릴리스 변경사항"을 참조하십시오.

절차

- 1 대상 서버에 **root**로 로그인합니다.

- 2 설치 파일을 대상 서버에 다운로드합니다.

미디어에 있는 소프트웨어를 구입한 경우에는 대상 서버가 액세스할 수 있는 위치에 설치 파일을 복사하십시오.

- 3 다운로드의 체크섬이 다운로드 페이지에 게시된 체크섬과 일치하는지 확인합니다.

MD5 및 SHA1의 체크섬 값이 다운로드 페이지에 게시되어 있습니다. 적절한 도구를 사용하여 다운로드한 설치 파일의 체크섬이 다운로드 페이지에 표시된 체크섬과 일치하는지 확인합니다. 다음 형식의 Linux 명령은 *installation-file*에 대한 체크섬을 표시합니다.

```
[root@cell11 /tmp]# md5sum installation-file
```

이 명령은 설치 파일 체크섬을 반환하며, 이 값은 다운로드 페이지의 MD5 체크섬과 일치해야 합니다.

- 4 설치 파일을 실행할 수 있는지 확인합니다.

설치 파일은 **실행** 권한이 있어야 실행할 수 있습니다. 이 권한이 있는지 확인하려면 콘솔, 셸 또는 터미널 창을 열고 다음 Linux 명령을 실행합니다. 명령에서 *installation-file*은 VMware Cloud Director 설치 파일의 전체 경로 이름입니다.

```
[root@cell11 /tmp]# chmod u+x installation-file
```

- 5 콘솔, 셸 또는 터미널 창에서 `--private-key-path` 옵션 및 대상 셸의 개인 키에 대한 경로 이름과 함께 설치 파일을 실행합니다.

데이터베이스 upgrade 유틸리티의 다른 명령 옵션을 추가할 수 있습니다.

```
./installation-file --private-key-path /vcloud/.ssh/id_rsa
```

참고 공백이 포함된 디렉터리가 해당 경로 이름에 있는 설치 파일은 실행할 수 없습니다.

설치 관리자는 이전 버전의 VMware Cloud Director를 감지하고 업그레이드를 확인하라는 메시지를 표시합니다.

설치 관리자가 설치 파일의 버전과 같거나 이후 버전인 VMware Cloud Director를 감지하면 오류 메시지가 표시되고 종료됩니다.

- 6 **y**를 입력하고 Enter 키를 눌러서 업그레이드를 확인합니다.

결과

설치 관리자에서 다음과 같은 다중 셸 업그레이드 워크플로가 시작됩니다.

- 1 현재 셸 호스트가 모든 요구 사항을 충족하는지 확인합니다.
- 2 VMware Cloud Director RPM 패키지의 압축을 풉니다.
- 3 현재 셸에서 VMware Cloud Director 소프트웨어를 업그레이드합니다.
- 4 VMware Cloud Director 데이터베이스를 업그레이드합니다.
- 5 나머지 셸 각각에서 VMware Cloud Director 소프트웨어를 업그레이드한 다음 해당 셸에서 VMware Cloud Director 서비스를 다시 시작합니다.
- 6 현재 셸에서 VMware Cloud Director 서비스를 다시 시작합니다.

다음에 수행할 작업

서버 그룹의 모든 셸에서 VMware Cloud Director 서비스를 시작합니다.

이제 연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager 업그레이드 작업을 수행한 다음 vCenter Server 시스템, ESXi 호스트 및 NSX Edge 업그레이드 작업을 수행할 수 있습니다.

수동으로 VMware Cloud Director 설치를 업그레이드

명령 옵션 없이 VMware Cloud Director 설치 관리자를 실행하여 단일 셸을 업그레이드할 수 있습니다. 업그레이드된 셸을 다시 시작하기 전에 데이터베이스 스키마를 업그레이드해야 합니다. 서버 그룹에서 적어도 하나의 셸을 업그레이드한 후 데이터베이스 스키마를 업그레이드합니다.

지원되는 Linux OS에서 Linux용 VMware Cloud Director 설치 관리자를 사용하여 VMware Cloud Director 설치로 구성된 VMware Cloud Director 서버 그룹을 업그레이드할 수 있습니다. VMware Cloud Director 서버 그룹이 VMware Cloud Director 9.5 장치 배포로 구성된 경우, Linux용 VMware Cloud Director 설치 관리자를 사용하여 마이그레이션 워크플로의 일부로만 기존 환경을 업그레이드합니다. **VMware Cloud Director 장치 업그레이드 및 마이그레이션**의 내용을 참조하십시오.

다중 셀 VMware Cloud Director 설치의 경우 각 셀과 데이터베이스를 수동으로 차례로 업그레이드하는 대신 VMware Cloud Director 설치의 오케스트레이션된 업그레이드를 수행할 수 있습니다. [VMware Cloud Director 설치의 오케스트레이션된 업그레이드를 수행의 내용을 참조하십시오.](#)

사전 요구 사항

- VMware Cloud Director 데이터베이스, vSphere 구성 요소 및 NSX 구성 요소가 VMware Cloud Director의 새 버전과 호환되는지 확인합니다.

중요 기존 VMware Cloud Director 설치에서 Oracle 데이터베이스 또는 Microsoft SQL Server 데이터베이스를 사용하는 경우 업그레이드 전에 PostgreSQL 데이터베이스로 마이그레이션했는지 확인합니다. 가능한 업그레이드 경로는 [Linux에서 VMware Cloud Director 업그레이드의 내용을 참조하십시오.](#)

- VMware Cloud Director 서버 그룹에 있는 서버에 대한 슈퍼유저 자격 증명이 있는지 확인합니다.
- 설치 관리자에서 설치 파일의 디지털 서명을 확인하려면 대상 서버에 VMware 공용 키를 다운로드하여 설치합니다. 설치 파일의 디지털 서명을 이미 확인한 경우 설치 중에 다시 확인할 필요가 없습니다. [VMware 공용 키 다운로드 및 설치의 내용을 참조하십시오.](#)
- 업그레이드할 버전의 VMware Cloud Director 소프트웨어를 사용할 수 있는 유효한 라이선스 키가 있는지 확인합니다.
- 모든 ESXi 호스트가 활성화되었는지 확인합니다. 비활성화된 ESXi 호스트는 지원되지 않습니다.

절차

1 VMware Cloud Director 셀 업그레이드

VMware Cloud Director 설치 관리자는 대상 서버가 모든 업그레이드 전제 조건을 충족하는지 확인한 후 해당 서버의 VMware Cloud Director 소프트웨어를 업그레이드합니다.

2 VMware Cloud Director 데이터베이스 업그레이드

업그레이드된 VMware Cloud Director 서버에서 VMware Cloud Director 데이터베이스를 업그레이드하는 도구를 실행합니다. 공유 데이터베이스를 업그레이드하기 전에 업그레이드된 VMware Cloud Director 서버를 다시 시작하지 말아야 합니다.

다음에 수행할 작업

- 서버 그룹 및 데이터베이스의 모든 VMware Cloud Director 서버를 업그레이드한 후 모든 셀에서 VMware Cloud Director 서비스를 시작할 수 있습니다.
- 연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager 업그레이드
- 각 NSX Manager를 업그레이드한 후에 vCenter Server 시스템, 호스트 및 NSX Edge를 업그레이드할 수 있습니다. [vCenter Server 시스템, ESXi 호스트 및 NSX Edge 업그레이드의 내용을 참조하십시오.](#)

VMware Cloud Director 셀 업그레이드

VMware Cloud Director 설치 관리자는 대상 서버가 모든 업그레이드 전제 조건을 충족하는지 확인한 후 해당 서버의 VMware Cloud Director 소프트웨어를 업그레이드합니다.

Linux용 VMware Cloud Director는 `vmware-vcloud-director-distribution-v.v.v-
"nnnnnn".bin` 형식의 이름을 가지는 디지털 서명된 실행 파일로 배포됩니다. 여기서 `v.v.v`는 제품 버전을 나타내고 `"nnnnnn"`은 빌드 번호를 나타냅니다. 예를 들면 `vmware-vcloud-director-distribution-8.10.0-3698331.bin`과 같습니다. 이 실행 파일을 실행하면 VMware Cloud Director가 설치 또는 업그레이드됩니다.

다중 셀 VMware Cloud Director 설치의 경우 VMware Cloud Director 서버 그룹의 각 구성원에서 VMware Cloud Director 설치 관리자를 실행해야 합니다.

절차

- 1 대상 서버에 **root**로 로그인합니다.

- 2 설치 파일을 대상 서버에 다운로드합니다.

미디어에 있는 소프트웨어를 구입한 경우에는 대상 서버가 액세스할 수 있는 위치에 설치 파일을 복사하십시오.

- 3 다운로드의 체크섬이 다운로드 페이지에 게시된 체크섬과 일치하는지 확인합니다.

MD5 및 SHA1의 체크섬 값이 다운로드 페이지에 게시되어 있습니다. 적절한 도구를 사용하여 다운로드한 설치 파일의 체크섬이 다운로드 페이지에 표시된 체크섬과 일치하는지 확인합니다. 다음 형식의 Linux 명령은 *installation-file*에 대한 체크섬을 표시합니다.

```
[root@cell11 /tmp]# md5sum installation-file
```

이 명령은 설치 파일 체크섬을 반환하며, 이 값은 다운로드 페이지의 MD5 체크섬과 일치해야 합니다.

- 4 설치 파일을 실행할 수 있는지 확인합니다.

설치 파일은 **실행** 권한이 있어야 실행할 수 있습니다. 이 권한이 있는지 확인하려면 콘솔, 셸 또는 터미널 창을 열고 다음 Linux 명령을 실행합니다. 명령에서 *installation-file*은 VMware Cloud Director 설치 파일의 전체 경로 이름입니다.

```
[root@cell11 /tmp]# chmod u+x installation-file
```

- 5 설치 파일을 실행합니다.

설치 파일을 실행하려면 다음과 같이 전체 경로 이름을 입력합니다.

```
[root@cell11 /tmp]# ./installation-file
```

이 파일에는 설치 스크립트와 내장된 RPM 패키지가 포함되어 있습니다.

참고 공백이 포함된 디렉터리가 해당 경로 이름에 있는 설치 파일은 실행할 수 없습니다.

설치 관리자가 설치 파일의 버전과 같거나 이후 버전인 VMware Cloud Director를 감지하면 오류 메시지가 표시되고 종료됩니다.

설치 관리자가 이전 버전의 VMware Cloud Director를 감지하면 업그레이드를 확인하라는 메시지가 표시됩니다.

6 y를 입력하고 Enter 키를 눌러서 업그레이드를 확인합니다.

설치 관리자에서 다음과 같은 업그레이드 워크플로가 시작됩니다.

- a 호스트가 모든 요구 사항을 충족하는지 확인합니다.
- b VMware Cloud Director RPM 패키지의 압축을 풉니다.
- c 셸에서 모든 활성 VMware Cloud Director 작업이 끝나면 서버의 VMware Cloud Director 서비스를 중지하고, 설치되어 있는 VMware Cloud Director 소프트웨어를 업그레이드합니다.

대상 서버에 VMware 공용 키를 설치하지 않은 경우에는 설치 관리자에 다음과 같은 형식의 경고가 표시됩니다.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

대상 서버에서 기존 global.properties 파일을 변경하는 경우에는 설치 관리자에 다음과 같은 형식의 경고가 표시됩니다.

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

참고 기존 global.properties 파일을 이전에 업데이트한 경우에는 global.properties.rpmnew에서 변경 사항을 검색할 수 있습니다.

7 (선택 사항) 로깅 속성을 업데이트합니다.

업그레이드를 완료하면 /opt/vmware/vcloud-director/etc/log4j.properties.rpmnew 파일에 새 로깅 속성이 기록됩니다.

옵션	작업
기존 로깅 속성을 변경하지 않은 경우	이 파일을 /opt/vmware/vcloud-director/etc/log4j.properties에 복사합니다.
로깅 속성을 변경한 경우	변경 내용을 유지하려면 /opt/vmware/vcloud-director/etc/log4j.properties.rpmnew를 기존 /opt/vmware/vcloud-director/etc/log4j.properties 파일과 병합합니다.

결과

VMware Cloud Director 업그레이드가 끝나면 설치 관리자에 이전 구성 파일의 위치에 대한 정보가 포함된 메시지가 표시됩니다. 그런 다음 설치 관리자에 데이터베이스 업그레이드 도구를 실행하라는 메시지가 표시됩니다.

다음에 수행할 작업

아직 업그레이드하지 않은 경우 VMware Cloud Director 데이터베이스를 업그레이드할 수 있습니다.

서버 그룹의 각 VMware Cloud Director 셀에서 이 절차를 반복합니다.

중요 서버 그룹 및 데이터베이스의 모든 셀을 업그레이드할 때까지 VMware Cloud Director 서비스를 시작하지 마십시오.

VMware Cloud Director 데이터베이스 업그레이드

업그레이드된 VMware Cloud Director 서버에서 VMware Cloud Director 데이터베이스를 업그레이드하는 도구를 실행합니다. 공유 데이터베이스를 업그레이드하기 전에 업그레이드된 VMware Cloud Director 서버를 다시 시작하지 말아야 합니다.

실행 중인 모든 작업 및 최근에 완료된 작업에 대한 정보는 VMware Cloud Director 데이터베이스에 저장됩니다. 데이터베이스를 업그레이드하면 이 작업 정보가 무효화되기 때문에 데이터베이스 업그레이드 유틸리티는 업그레이드 프로세스를 시작할 때 실행 중인 작업이 없는지 확인합니다.

VMware Cloud Director 서버 그룹의 모든 셀은 동일한 데이터베이스를 공유합니다. 업그레이드하는 셀의 수에 관계없이 데이터베이스는 한 번만 업그레이드합니다. 데이터베이스가 업그레이드되면 업그레이드되지 않은 VMware Cloud Director 셀은 데이터베이스에 연결할 수 없습니다. 업그레이드된 데이터베이스에 연결되도록 모든 셀을 업그레이드해야 합니다.

사전 요구 사항

- 데이터베이스 소프트웨어 벤더에서 권장하는 절차를 사용하여 기존 데이터베이스를 백업합니다.
- 서버 그룹의 모든 VMware Cloud Director 셀이 중지되어 있는지 확인합니다. 업그레이드된 셀은 업그레이드 프로세스를 수행하는 동안 중지됩니다. 아직 업그레이드되지 않은 VMware Cloud Director 서버가 있는 경우 셀 관리 도구를 사용하여 해당 서비스를 정지하고 종료합니다. 셀 관리 도구를 사용하여 셀을 관리하는 방법에 대한 자세한 내용은 [장 5 셀 관리 도구 참조 사항](#)의 내용을 참조하십시오.
- 데이터베이스 업그레이드 유틸리티 참조 항목을 검토합니다.

절차

- 1 데이터베이스 upgrade 유틸리티를 옵션을 사용하거나 사용하지 않고 실행합니다.

```
/opt/vmware/vcloud-director/bin/upgrade
```

데이터베이스 업그레이드 유틸리티에서 호환되지 않는 NSX Manager 버전이 감지되면 경고 메시지가 표시되고 업그레이드가 취소됩니다.

- 2 프롬프트에 **y**를 입력하고 Enter 키를 눌러서 데이터베이스 업그레이드를 확인합니다.
- 3 프롬프트에 **y**를 입력하고 Enter 키를 눌러서 데이터베이스를 백업했음을 확인합니다.

--backup-completed 옵션을 사용하면 유틸리티에서 이 프롬프트를 건너뛵니다.

- 4 유틸리티가 활성 셀을 감지하면 계속할 것인지 묻는 프롬프트에서 **n**을 입력하여 셀을 종료한 다음 실행 중인 셀이 없는지 확인하고 **단계 1**단계의 업그레이드를 다시 시도합니다.

결과

데이터베이스 업그레이드 도구가 실행되고 진행률 메시지가 표시됩니다. 업그레이드가 완료되면 현재 서버에서 VMware Cloud Director 서비스를 시작하라는 메시지가 표시됩니다.

다음에 수행할 작업

y를 입력하고 Enter 키를 누르거나 나중에 `service vmware-vcd start` 명령을 실행하여 서비스를 시작합니다.

업그레이드된 VMware Cloud Director 서버의 서비스를 시작할 수 있습니다.

서버 그룹의 나머지 VMware Cloud Director 구성원을 업그레이드하고 해당 서비스를 시작할 수 있습니다. [VMware Cloud Director 셀 업그레이드](#)의 내용을 참조하십시오.

데이터베이스 업그레이드 유틸리티 참조

upgrade 유틸리티를 실행하는 경우 명령줄에 설치 정보를 옵션 및 인수로 제공합니다.

upgrade 유틸리티의 위치는 `/opt/vmware/vcloud-director/bin/`입니다.

표 4-3. 데이터베이스 업그레이드 유틸리티 옵션 및 인수

옵션	인수	설명
<code>--backup-completed</code>	없음	VMware Cloud Director 백업을 완료했음을 지정합니다. 이 옵션을 포함하면 업그레이드 유틸리티가 데이터베이스를 백업하라는 메시지를 표시하지 않습니다.
<code>--ceip-user</code>	CEIP 서비스 계정의 사용자 이름입니다.	이 사용자 이름을 사용하는 사용자가 시스템 조직에 이미 있으면, 업그레이드가 실패합니다. 기본값: <code>phone-home-system-account</code> .

표 4-3. 데이터베이스 업그레이드 유틸리티 옵션 및 인수 (계속)

옵션	인수	설명
--enable-ceip	다음 중 하나를 선택합니다. ■ true ■ false	이 설치에서 VMware CEIP(고객 환경 향상 프로그램)에 참여할지 지정합니다. 값을 제공하지 않고 현재 구성에서 false로 설정하지 않는 경우 기본적으로 true로 설정됩니다. VMware CEIP(고객 환경 향상 프로그램)은 CEIP를 통해 수집된 데이터에 대한 추가 정보를 제공합니다. VMware에서 이러한 정보를 사용하는 목적은 Trust & Assurance Center(http://www.vmware.com/trustvmware/ceip.html)에 명시되어 있습니다. 셀 관리 도구를 사용하여 언제든지 이 제품에 대해 VMware의 CEIP에 참여하거나 탈퇴할 수 있습니다. 장 5 셀 관리 도구 참조 사항 의 내용을 참조하십시오.
--installer-path	VMware Cloud Director 설치 파일의 전체 경로 이름입니다. 설치 파일 및 이 파일이 저장된 디렉터리를 vcloud.vcloud 사용자가 읽을 수 있어야 합니다.	--private-key-path 옵션이 필요합니다.
--maintenance-cell	IP 주소	업그레이드하는 동안 업그레이드 유틸리티가 유지 보수 모드로 실행할 셀의 IP 주소입니다. 이 셀은 다른 셀이 종료되기 전에 유지 보수 모드로 설정되며 다른 셀이 업그레이드되는 동안 유지 보수 모드로 남아 있습니다. 이 셀은 다른 셀이 업그레이드되고 그 중 하나 이상이 다시 시작된 후에 종료되고 업그레이드됩니다. --private-key-path 옵션이 필요합니다.
--multisite-user	다중 사이트 시스템 계정의 사용자 이름입니다.	이 계정은 VMware Cloud Director 다중 사이트 기능에 사용됩니다. 이 사용자 이름을 사용하는 사용자가 시스템 조직에 이미 있으면, 업그레이드가 실패합니다. 기본값: multisite-system-account.

표 4-3. 데이터베이스 업그레이드 유틸리티 옵션 및 인수 (계속)

옵션	인수	설명
--private-key-path	경로 이름	셀의 개인 키에 대한 전체 경로 이름입니다. 이 옵션을 사용하면 데이터베이스가 업그레이드된 후 서버 그룹 내의 모든 셀이 정상적으로 종료되고, 업그레이드되고, 다시 시작됩니다. 이 업그레이드 워크플로에 대한 자세한 정보는 VMware Cloud Director 설치의 오케스트레이션된 업그레이드를 수행의 내용을 참조하십시오.
--unattended-upgrade	없음	자동 업그레이드를 지정합니다.

--private-key-path 옵션을 사용하는 경우 암호 없이 슈퍼 사용자의 ssh 연결을 허용하도록 모든 셀을 구성해야 합니다. 여기에 나와 있는 것과 같은 Linux 명령을 사용하여 이를 확인할 수 있습니다. 이 예제에서는 ID를 vcloud로 설정한 다음 루트 암호를 제공하지 않고 *cell-ip*에 있는 셀에 root로 ssh 연결을 시도합니다.

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

로컬 셀의 *private-key-path*에 있는 개인 키를 vcloud.vcloud 사용자가 읽을 수 있고, 해당하는 공용 키가 *cell-ip*에서 루트 사용자의 authorized-keys 파일에 추가되어 있으면 명령이 성공합니다.

참고 VMware Cloud Director 프로세스가 실행되는 ID로 사용할 vcloud 사용자, vcloud 그룹 및 vcloud.vcloud 계정이 VMware Cloud Director 설치 관리자에 의해 생성됩니다. vcloud 사용자는 암호가 없습니다.

VMware Cloud Director 업그레이드 후 작업

모든 VMware Cloud Director 서버 및 공유 데이터베이스를 업그레이드한 후에는 클라우드에 네트워크 서비스를 제공하는 NSX Manager 인스턴스를 업그레이드할 수 있습니다. 그런 다음, VMware Cloud Director 설치에 등록되어 있는 vCenter Server 인스턴스 및 ESXi 호스트를 업그레이드할 수 있습니다.

중요 VMware Cloud Director는 고급 Edge 게이트웨이만 지원합니다. 고급이 아닌 레거시 Edge 게이트웨이는 고급 게이트웨이로 변환해야 합니다. <https://kb.vmware.com/kb/66767>의 내용을 참조하십시오.

버전 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고, 서버 ID를 SSL 핸드셰이크의 일부로 확인할 수 있습니다. VMware Cloud Director 네트워크 연결을 보호하려면 연결 테스트를 위해 VMware Cloud Director API를 사용하는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성합니다. VMware Cloud Director 설치 또는 업그레이드 후 그리고 테넌트에 VMware Cloud Director에 대한 액세스 권한을 부여하기 전에 거부 목록을 구성합니다. **테스트 연결 거부 목록 구성**의 내용을 참조하십시오.

중요 버전 10.1 이상으로 업그레이드한 후 VMware Cloud Director는 연결된 모든 인프라 끝점에 대한 인증서를 항상 확인합니다. 이는 VMware Cloud Director가 SSL 인증서를 관리하는 방식이 변경되었기 때문입니다. 업그레이드 전에 인증서를 VMware Cloud Director로 가져오지 않으면 SSL 확인 문제로 인해 vCenter Server 및 NSX 연결에 실패한 연결 오류가 표시될 수 있습니다. 이 경우 업그레이드 후 다음 두 가지 옵션이 제공됩니다.

- 1 셸 관리 도구 `trust-infra-certs` 명령을 실행하여 모든 인증서를 중앙 집중식 인증서 저장소로 자동으로 가져옵니다. **vSphere 리소스에서 끝점 인증서 가져오기**를 참조하십시오.
- 2 Service Provider Admin Portal UI에서 각 vCenter Server 및 NSX 인스턴스를 선택하고 인증서를 수락하는 동안 자격 증명을 다시 입력합니다.

연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager 업그레이드

VMware Cloud Director에 등록된 ESXi 호스트와 vCenter Server를 업그레이드하기 전에 해당 vCenter Server에 연결된 각 NSX Manager를 업그레이드해야 합니다.

NSX Manager를 업그레이드하면 NSX 관리 기능에 대한 액세스가 중단되지만 네트워크 서비스는 중단되지 않습니다. VMware Cloud Director 셸이 실행 중인지 여부에 관계없이 VMware Cloud Director 업그레이드를 전후하여 NSX Manager를 업그레이드할 수 있습니다.

NSX 업그레이드에 대한 자세한 내용은 <https://docs.vmware.com>의 NSX for vSphere 설명서를 참조하십시오.

절차

- 1 VMware Cloud Director 설치에 등록된 각 vCenter Server에 연결되어 있는 NSX Manager를 업그레이드합니다.
- 2 모든 NSX Manager를 업그레이드한 후에는 등록된 vCenter Server 시스템과 ESXi 호스트를 업그레이드할 수 있습니다.

vCenter Server 시스템, ESXi 호스트 및 NSX Edge 업그레이드

VMware Cloud Director 및 NSX Manager를 업그레이드한 후에는 VMware Cloud Director에 등록되어 있는 vCenter Server 시스템 및 ESXi 호스트를 업그레이드해야 합니다. 연결된 모든 vCenter Server 시스템과 ESXi 호스트를 업그레이드한 후에 NSX Edge를 업그레이드할 수 있습니다.

사전 요구 사항

클라우드에 연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager를 이미 업그레이드했는지 확인합니다. 연결된 vCenter Server 시스템과 연결되어 있는 각 NSX Manager 업그레이드의 내용을 참조하십시오.

절차

- 1 vCenter Server 인스턴스를 비활성화합니다.
 - a VMware Cloud Director Service Provider Admin Portal의 위쪽 탐색 모음의 **리소스**에서 **vSphere 리소스**를 선택합니다.
 - b 왼쪽 패널에서 **vCenter Server 인스턴스**를 클릭합니다.
 - c 비활성화할 vCenter Server 인스턴스 옆에 있는 라디오 버튼을 선택하고 **사용 안 함**을 클릭합니다.
 - d **확인**을 클릭합니다.
- 2 vCenter Server 시스템을 업그레이드합니다.
자세한 내용은 "vCenter Server 업그레이드"를 참조하십시오.
- 3 모든 VMware Cloud Director 공용 URL 및 인증서 체인을 확인합니다.
 - a 위쪽 탐색 모음에서 **관리**를 선택합니다.
 - b 왼쪽 패널의 **설정** 아래에서 **공개 주소**를 클릭합니다.
 - c 모든 공개 주소를 확인합니다.
- 4 VMware Cloud Director에서 vCenter Server 등록을 새로 고칩니다.
 - a VMware Cloud Director Service Provider Admin Portal의 위쪽 탐색 모음의 **리소스**에서 **vSphere 리소스**를 선택합니다.
 - b 왼쪽 패널에서 **vCenter Server 인스턴스**를 클릭합니다.
 - c 대상 vCenter Server 옆에 있는 라디오 버튼을 선택하고 **다시 연결**을 클릭합니다.
 - d **확인**을 클릭합니다.
- 5 업그레이드된 vCenter Server 시스템이 지원하는 각 ESXi 호스트를 업그레이드합니다.
"VMware ESXi 업그레이드"를 참조하십시오.

중요 클라우드에 속한 가상 시스템을 지원할 정도로 업그레이드된 호스트의 용량이 충분한지 확인하려면 호스트를 몇 개씩 업그레이드하십시오. 이렇게 하면 Host Agent 업그레이드를 지정된 시간에 완료하여 가상 시스템을 업그레이드된 호스트로 다시 마이그레이션할 수 있습니다.

- a vCenter Server 시스템을 사용하여 호스트를 유지 보수 모드로 설정하고, 해당 호스트의 모든 가상 시스템을 다른 호스트에 마이그레이션할 수 있도록 허용합니다.
- b 호스트를 업그레이드합니다.

c vCenter Server 시스템을 사용하여 호스트를 다시 연결합니다.

d vCenter Server 시스템을 사용하여 호스트의 유지 보수 모드를 해제합니다.

- 6 (선택 사항) 업그레이드된 vCenter Server 시스템과 연결된 NSX Manager에서 관리하는 NSX Edge를 업그레이드합니다.

NSX Edge를 업그레이드하면 성능과 통합이 향상됩니다. NSX Manager 또는 VMware Cloud Director를 사용하여 NSX Edge를 업그레이드할 수 있습니다.

- NSX Manager를 사용하여 NSX Edge 업그레이드에 대한 자세한 내용은 <https://docs.vmware.com/kr/>의 NSX for vSphere 설명서를 참조하십시오.
- VMware Cloud Director를 사용하여 NSX Edge 게이트웨이를 업그레이드하려면 Edge에서 지원하는 VMware Cloud Director 네트워크 개체에서 작업해야 합니다.
 - VMware Cloud Director 또는 VMware Cloud Director API를 사용하여 Edge 게이트웨이가 서비스하는 네트워크를 재설정할 경우 Edge 게이트웨이가 자동으로 적절하게 업그레이드됩니다.
 - Edge 게이트웨이를 재배포하면 연결된 NSX Edge 어플라이언스가 업그레이드됩니다.

참고 다시 배포는 NSX Data Center for vSphere Edge 게이트웨이에만 지원됩니다.

- vApp의 컨텍스트 내에서 vApp 네트워크를 재설정하면 해당 네트워크와 연결된 NSX Edge 어플라이언스가 업그레이드됩니다. vApp 컨텍스트 내에서 vApp 네트워크를 재설정하려면 vApp의 **네트워크** 탭으로 이동하여 해당 네트워킹 세부 정보를 표시하고 vApp 네트워크 이름 옆에 있는 라디오 버튼을 클릭한 후 **재설정**을 클릭합니다.

Edge 게이트웨이 다시 배포 및 vApp 네트워크 재설정 방법에 대한 자세한 내용은 "VMware Cloud Director API 프로그래밍 가이드"의 내용을 참조하십시오.

다음에 수행할 작업

VMware Cloud Director 설치 환경에 등록된 다른 vCenter Server 시스템에 대해 이 절차를 반복합니다.

셀 관리 도구 참조 사항

5

셀 관리 도구는 VMware Cloud Director 셀 또는 데이터베이스를 관리하는 데 사용할 수 있는 명령줄 유틸리티입니다. 대부분의 작업에는 슈퍼 사용자 또는 시스템 관리자 자격 증명이 필요합니다.

셀 관리 도구는 /opt/vmware/vcloud-director/bin/에 설치됩니다. 이 명령을 사용하여 단일 명령을 실행하거나 대화형 셀로 실행할 수 있습니다.

사용 가능한 명령 나열

사용 가능한 셀 관리 도구 명령을 나열하려면 다음 명령줄을 사용하십시오.

```
./cell-management-tool -h
```

셀 모드 사용

여기에 표시된 것처럼 셀 관리 도구를 인수 없이 호출하여 대화형 셀로 실행할 수 있습니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]#./Cell-management-tool
Cell Management Tool v8.14.0.4146350 Type "help" for available subcommands. cmt>
```

셀 모드에서는 이 예제와 같이 cmt> 프롬프트에서 모든 셀 관리 도구 명령을 입력할 수 있습니다.

```
cmt>cell -h
usage: cell [options] -a,--application-states display the state of each application on the
cell [DEPRECATED - use the cell-application command instead] -h,--help print this message
-i,--pid <arg> the process id of the cell [REQUIRED if username is not specified] -m,--
maintenance <arg> gracefully enter maintenance mode on the cell -p,--password <arg>
administrator password [OPTIONAL] -q,--quiesce <arg> quiesce activity on the cell -s,--
shutdown gracefully shutdown the cell -t,--status display activity on the cell -tt,--status-
verbose display a verbose description of activity on the cell -u,--username <arg>
administrator username [REQUIRED if pid is not specified] Note: You will be prompted for
administrator password if not entered in command line. cmt>
```

이 명령은 실행이 끝나면 cmt> 프롬프트로 돌아갑니다. 셀 모드를 종료하려면 cmt> 프롬프트에서 **exit**를 입력하십시오.

예제: 셀 관리 도구 사용 도움말

이 예제는 사용 가능한 셀 관리 도구 명령을 나열하는 비대화형 단일 명령을 실행합니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool -h,--help print this message Available commands: cell -
Manipulates the Cell and core components certificates - Reconfigures the SSL certificates for
the cell . . . For command specific help: cell-management-tool <commandName> -h
```

■ VMware Cloud Director 설치 구성

시스템 관리자 계정 및 관련 정보와 함께 셀 관리 도구의 `system-setup` 명령을 사용하여 서버 그룹의 데이터베이스를 초기화합니다.

■ 레거시 API 끝점에 대한 서비스 제공자 액세스 비활성화

VMware Cloud Director 10.0부터는 서비스 제공자와 테넌트가 VMware Cloud Director에 액세스하는 데 별도의 VMware Cloud Director OpenAPI 로그인 끝점을 사용할 수 있습니다.

■ 셀 관리

셀 관리 도구의 `cell` 하위 명령을 사용하여 새 작업을 시작하지 못하도록 작업 스케줄러를 일시 중단하거나, 활성 작업의 상태를 살펴보거나, 셀 유지 보수 모드를 제어하거나, 셀을 정상적으로 종료할 수 있습니다.

■ 셀 애플리케이션 관리

셀 관리 도구의 `cell-application` 명령을 사용하여 셀이 시작 시 실행하는 애플리케이션 집합을 제어합니다.

■ 데이터베이스 연결 속성 업데이트

셀 관리 도구의 `reconfigure-database` 하위 명령을 사용하여 VMware Cloud Director 데이터베이스의 연결 속성을 업데이트할 수 있습니다.

■ 손상된 스케줄러 데이터 검색 및 복구

VMware Cloud Director는 Quartz 작업 스케줄러를 사용하여 시스템에서 실행 중인 비동기 작업을 조정합니다. Quartz 스케줄러 데이터베이스가 손상되면 시스템을 정지하지 못할 수 있습니다. 셀 관리 도구의 `fix-scheduler-data` 명령을 사용하여 데이터베이스에서 손상된 스케줄러 데이터를 검색하고 필요한 경우 해당 데이터를 복구할 수 있습니다.

■ HTTPS 및 콘솔 프록시 끝점에 대한 자체 서명된 인증서 생성

셀 관리 도구의 `generate-certs` 명령을 사용하여 HTTPS 및 콘솔 프록시 끝점에 대한 자체 서명된 SSL 인증서를 생성합니다.

■ HTTPS 및 콘솔 프록시 끝점에 대한 인증서 바꾸기

셀 관리 도구의 `certificates` 명령을 사용하여 HTTPS 및 콘솔 프록시 끝점에 대한 SSL 인증서를 바꿉니다.

■ 외부 서비스에서 SSL 인증서 가져오기

셀 관리 도구의 `import-trusted-certificates` 명령을 사용하여 AMQP 및 VMware Cloud Director 데이터베이스와 같은 외부 서비스에 대한 보안 연결 설정에 사용할 인증서를 가져옵니다.

■ vSphere 리소스에서 끝점 인증서 가져오기

업그레이드 후 셀 관리 도구의 `trust-infra-certs` 명령을 사용하여 환경의 vSphere 리소스에서 VMware Cloud Director 데이터베이스로 인증서를 수집하고 가져옵니다.

■ 테스트 연결 거부 목록 구성

설치 또는 업그레이드 후에는 VMware Cloud Director 네트워크에 대한 액세스 권한을 테넌트에게 제공하기 전에 먼저 셀 관리 도구의 `manage-test-connection-blacklist` 명령을 사용하여 내부 호스트에 대한 액세스를 차단합니다.

■ 모든 활성 셀의 FIPS 상태 보기

VMware Cloud Director 10.2.2부터 모든 활성 VMware Cloud Director 셀의 FIPS 상태를 확인하기 위해 `fips-status` 명령을 사용할 수 있습니다. 이 명령은 VMware Cloud Director 장치의 FIPS 상태를 표시하지 않습니다.

■ 허용되는 SSL 암호화 목록 관리

셀 관리 도구의 `ciphers` 명령을 사용하여 SSL 핸드셰이크 프로세스 도중 사용하기 위해 셀이 제공하는 암호화 스위트 집합을 구성합니다.

■ 허용되는 SSL 프로토콜 목록 관리

SSL 핸드셰이크 프로세스 중에 사용하도록 셀이 제공하는 SSL 프로토콜 집합을 구성하려면 셀 관리 도구의 `ssl-protocols` 명령을 사용합니다.

■ 메트릭 수집 및 게시 구성

셀 관리 도구의 `configure-metrics` 명령을 사용하여 수집할 메트릭 집합을 구성할 수 있습니다.

■ Cassandra 메트릭 데이터베이스 구성

셀 관리 도구의 `cassandra` 명령을 사용하여 셀을 메트릭 데이터베이스(선택 사항)에 연결합니다.

■ 시스템 관리자 암호 복구

VMware Cloud Director 데이터베이스 사용자 이름과 암호를 아는 경우 셀 관리 도구의 `recover-password` 명령을 사용하여 VMware Cloud Director 시스템 관리자 암호를 복구할 수 있습니다.

■ 작업의 실패 상태 업데이트

셀이 고의로 종료되었을 때 실행 중이던 작업과 연관된 완료 상태를 업데이트하려면 셀 관리 도구의 `fail-tasks` 명령을 사용합니다. `fail-tasks` 명령은 모든 셀이 종료된 경우에만 사용할 수 있습니다.

■ 감사 메시지 처리 구성

셀 관리 도구의 `configure-audit-syslog` 명령을 사용하여 시스템이 감사 메시지를 기록하는 방식을 구성합니다.

■ e-메일 템플릿 구성

e-메일 경고를 만들 때 시스템에서 사용하는 템플릿을 관리하려면 셀 관리 도구의 `manage-email` 명령을 사용할 수 있습니다.

■ 연결이 끊어진 VM 찾기

셀 관리 도구의 `find-orphan-vms` 명령을 사용하여 vCenter 데이터베이스에는 있지만 VMware Cloud Director 데이터베이스에는 없는 가상 시스템에 대한 참조를 찾습니다.

■ VMware 고객 환경 항상 프로그램 참여 또는 탈퇴

VMware CEIP(고객 환경 항상 프로그램)에 참여하거나 탈퇴하려면 셀 관리 도구의 `configure-ceip` 하위 명령을 사용하면 됩니다.

■ 애플리케이션 구성 설정 업데이트

셀 관리 도구의 `manage-config` 하위 명령으로 카탈로그 임계치 조절 작업과 같은 다양한 애플리케이션 구성 설정을 업데이트할 수 있습니다.

■ 카탈로그 동기화 임계치 조절 구성

다른 조직에 게시되거나 다른 조직에서 구독된 카탈로그 항목이 많은 경우 카탈로그 동기화 중에 시스템 오버로드를 피하려면 카탈로그 동기화 임계치 조절을 구성하면 됩니다. 셀 관리 도구의 `manage-config` 하위 명령을 사용하여 동시에 동기화할 수 있는 라이브러리 항목 수를 제한하는 방식으로 카탈로그 동기화 임계치 조절을 구성할 수 있습니다.

■ VMware Cloud Director 사용자 인터페이스에 대한 액세스 실패 문제 해결

VMware Cloud Director 환경에서 VMware Cloud Director 셀의 유효한 IP 주소와 DNS 항목을 살펴보고 업데이트하려면 셀 관리 도구의 `manage-config` 하위 명령을 사용하면 됩니다.

■ vCenter VM 검색 디버깅

셀 관리 도구의 `debug-auto-import` 하위 명령을 사용하면 vApp을 검색하는 메커니즘이 하나 이상의 vCenter VM을 건너편 이유를 조사할 수 있습니다.

■ 다중 사이트에 스트레치된 네트워크에 대한 MAC 주소 재생성

동일한 설치 ID로 구성된 두 개의 VMware Cloud Director 사이트를 연결하는 경우에는 사이트 전반에 스트레치된 네트워크에서 MAC 주소 충돌이 발생할 수 있습니다. 이러한 충돌을 피하려면 설치 ID와는 다른 사용자 지정 시드를 기반으로 사이트 중 하나에서 MAC 주소를 재생성해야 합니다.

■ VMware Cloud Director 셀의 데이터베이스 IP 주소 업데이트

데이터베이스 고가용성 클러스터에서 VMware Cloud Director 셀의 IP 주소를 업데이트하려면 셀 관리 도구를 사용하면 됩니다.

VMware Cloud Director 설치 구성

시스템 관리자 계정 및 관련 정보와 함께 셀 관리 도구의 `system-setup` 명령을 사용하여 서버 그룹의 데이터베이스를 초기화합니다.

VMware Cloud Director 서버 그룹의 모든 서버를 구성하고 데이터베이스에 연결한 후에는 초기 시스템 관리자 계정을 생성하고 관련 정보와 함께 다음과 같은 형식의 명령줄을 사용하여 VMware Cloud Director 데이터베이스를 초기화할 수 있습니다.

```
cell-management-tool system-setup options
```

이미 설정된 시스템에서는 이 명령을 실행할 수 없습니다. --unattended 및 --password 를 제외한 모든 옵션을 지정해야 합니다.

표 5-1. 셀 관리 도구 옵션과 인수, system-setup 하위 명령

옵션	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
--email	생성 중인 시스템 관리자의 e-메일 주소.	시스템 관리자의 e-메일 주소는 VMware Cloud Director 데이터베이스에 저장됩니다.
--full-name	생성 중인 시스템 관리자의 전체 이름.	시스템 관리자의 전체 이름은 VMware Cloud Director 데이터베이스에 저장됩니다.
--installation-id	1에서 63 사이의 정수	이 VMware Cloud Director 설치에 대한 설치 ID. 시스템에서는 가상 NIC의 MAC 주소를 생성할 때 설치 ID를 사용합니다. 참고 다중 사이트 배포에서 VMware Cloud Director 설치 전반에 스트레치된 네트워크를 생성하려는 경우에는 각 VMware Cloud Director 설치에 대해 고유한 설치 ID를 설정하는 것이 좋습니다.
--password	생성 중인 시스템 관리자의 암호. --unattended 옵션을 사용할 때 필요합니다. --unattended 옵션을 사용하지 않는 경우 명령줄에 이 암호를 제공하지 않으면 암호를 입력하라는 메시지가 표시됩니다.	시스템 관리자는 VMware Cloud Director에 인증할 때 이 암호를 제공합니다.
--serial-number	이 설치를 위한 일련 번호(라이센스 키).	선택 사항입니다. 유효한 VMware Cloud Director 일련 번호여야 합니다.
--system-name	VMware Cloud Director vCenter Server 폴더의 이름을 사용하기 위한 이름.	이 VMware Cloud Director 설치는 등록하는 각 vCenter Server에서 이 이름의 폴더로 표시됩니다.

표 5-1. 셸 관리 도구 옵션과 인수, system-setup 하위 명령 (계속)

옵션	인수	설명
--unattended	없음	선택 사항입니다. 이 옵션과 함께 호출되면 명령에서 추가 입력을 요청하지 않습니다.
--user	생성 중인 시스템 관리자의 사용자 이름.	시스템 관리자는 VMware Cloud Director에 인증할 때 이 사용자 이름을 제공합니다.

예제: VMware Cloud Director 시스템 설정 지정

이와 같은 명령은 새 VMware Cloud Director 설치에 대한 모든 시스템 설정을 지정합니다.

--unattended 및 --password 가 지정되지 않았기 때문에 명령에서 시스템 관리자에 대해 생성할 암호를 제공하고 확인하라는 메시지를 표시합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool system-setup \ --user admin --full-name "VCD System
Administrator" --email vcd-admin@example.com --system-name VCD --installation-id 2
Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:

Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
Are you sure you want to use these parameters? [Y/n]:y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.
```

레거시 API 끝점에 대한 서비스 제공자 액세스 비활성화

VMware Cloud Director 10.0부터는 서비스 제공자와 테넌트가 VMware Cloud Director에 액세스하는 데 별도의 VMware Cloud Director OpenAPI 로그인 끝점을 사용할 수 있습니다.

새로운 OpenAPI 끝점 두 개를 사용하여 VMware Cloud Director에 대한 액세스를 제한함으로써 보안을 강화할 수 있습니다.

- /cloudapi/1.0.0/sessions/provider - 서비스 제공자 로그인을 위한 OpenAPI 끝점. 테넌트는 이 끝점을 사용하여 VMware Cloud Director에 액세스할 수 없습니다.
- /cloudapi/1.0.0/sessions/ - 테넌트 로그인을 위한 OpenAPI 끝점. 서비스 제공자는 이 끝점을 사용하여 VMware Cloud Director에 액세스할 수 없습니다.

기본적으로 제공자 관리자와 조직 사용자는 /api/sessions API 끝점에 로그인하여 VMware Cloud Director에 액세스할 수 있습니다.

셀 관리 도구의 `manage-config` 하위 명령을 사용하면 `/api/sessions` API 끝점에 대한 서비스 제공자 액세스를 비활성화하여, 제공자가 서비스 제공자만 액세스할 수 있는 새 `/cloudapi/1.0.0/sessions/provider` OpenAPI 끝점에 로그인하도록 제한할 수 있습니다.

참고 `/api/sessions` API 끝점에 대한 서비스 제공자 액세스를 비활성화하면 인증 헤더에 SAML 토큰만 제공하는 서비스 제공자 요청이 모든 레거시 API 끝점에 대해 실패합니다.

절차

- 1 VMware Cloud Director 셀의 OS에 **root**로 로그인하거나 SSH를 통해 연결합니다.
- 2 제공자가 `/api/sessions` API 끝점에 액세스할 수 없도록 차단하려면 셀 관리 도구를 사용하여 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v true
```

결과

서비스 제공자는 `/api/sessions` API 끝점에 더 이상 액세스할 수 없습니다. 서비스 제공자는 새 OpenAPI 끝점 `/cloudapi/1.0.0/sessions/provider`를 사용하여 VMware Cloud Director에 액세스할 수 있습니다. 테넌트는 `/api/sessions` API 끝점과 새 `/cloudapi/1.0.0/sessions/` OpenAPI 끝점 모두를 사용하여 VMware Cloud Director에 액세스할 수 있습니다.

다음에 수행할 작업

제공자가 `/api/sessions` API 끝점에 액세스할 수 있도록 설정하려면 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v false
```

셀 관리

셀 관리 도구의 `cell` 하위 명령을 사용하여 새 작업을 시작하지 못하도록 작업 스케줄러를 일시 중단하거나, 활성 작업의 상태를 살펴보거나, 셀 유지 보수 모드를 제어하거나, 셀을 정상적으로 종료할 수 있습니다.

셀을 관리하려면 명령줄에 다음과 같은 형식으로 명령을 입력하십시오.

```
cell-management-tool cell-usysadmin-username -p sysadmin-password option
```

여기서 *sysadmin-username*과 *sysadmin-password*는 **시스템 관리자**의 사용자 이름과 암호입니다.

참고 보안상의 이유로 암호를 생략할 수 있습니다. 이 경우 명령에 암호를 입력하라는 메시지가 표시되고 화면에는 암호가 표시되지 않습니다.

시스템 관리자 자격 증명을 제공하는 대신 `--pid` 옵션을 사용하여 셀 프로세스의 프로세스 ID를 제공할 수 있습니다. 셀의 프로세스 ID를 찾으려면 다음과 같은 명령을 사용하십시오.

```
cat /var/run/vmware-vcd-cell.pid
```

표 5-2. 셀 관리 도구 옵션과 인수, cell 하위 명령

옵션	인수	설명
<code>--help</code> (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--pid</code> (-i)	셀 프로세스의 프로세스 ID	<code>-username</code> 대신 이 옵션을 사용할 수 있습니다.
<code>--maintenance</code> (-m)	true 또는 false	셀을 유지 보수 모드로 설정합니다. true 인수는 셀의 활동을 정지하고 셀을 유지 보수 모드로 전환합니다. false 인수는 셀의 유지 보수 모드를 해제합니다.
<code>--password</code> (-p)	VMware Cloud Director 시스템 관리자 암호	<code>-username</code> 옵션을 사용할 경우 선택 사항입니다. 이 옵션을 생략하면 명령에 암호를 입력하라는 메시지가 표시되고 화면에는 암호가 표시되지 않습니다.
<code>--quiesce</code> (-q)	true 또는 false	셀의 활동을 정지합니다. true 인수는 스케줄러를 일시 중단합니다. false 인수는 스케줄러를 다시 시작합니다.
<code>--shutdown</code> (-s)	없음	서버에서 VMware Cloud Director 서비스가 정상적으로 종료됩니다.
<code>--status</code> (-t)	없음	셀에서 실행 중인 작업 수 및 셀의 상태에 대한 정보를 표시합니다.
<code>--status-verbose</code> (-tt)	없음	셀에서 실행 중인 작업 및 셀의 상태에 대한 자세한 정보를 표시합니다.
<code>--username</code> (-u)	VMware Cloud Director 시스템 관리자 사용자 이름	<code>-pid</code> 대신 이 옵션을 사용할 수 있습니다.

셀 애플리케이션 관리

셀 관리 도구의 `cell-application` 명령을 사용하여 셀이 시작 시 실행하는 애플리케이션 집합을 제어합니다.

VMware Cloud Director는 VMware Cloud Director 클라이언트에 필요한 서비스를 제공하는 여러 가지 애플리케이션을 실행합니다. 셀은 이러한 애플리케이션의 하위 집합을 기본적으로 시작합니다. 일반적으로 VMware Cloud Director 설치를 지원하려면 해당 하위 집합의 모든 구성원이 필요합니다.

셀이 시작될 때 실행되는 애플리케이션 목록을 보거나 변경하려면 다음 형식의 명령줄을 사용하십시오.

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell-application command
```

sysadmin-username

VMware Cloud Director 시스템 관리자의 사용자 이름입니다.

sysadmin-password

VMware Cloud Director 시스템 관리자의 암호입니다. 암호에 특수 문자가 포함된 경우에는 암호를 따옴표로 묶어야 합니다.

참고 `cell-management-tool` 명령줄에 VMware Cloud Director 시스템 관리자 암호를 지정할 수도 있지만 암호를 생략하는 것이 더 안전합니다. 그러면 `cell-management-tool`에 암호를 묻는 메시지가 표시되며, 암호 입력 시 화면에 암호가 표시되지 않습니다.

시스템 관리자 자격 증명을 제공하는 대신 `--pid` 옵션을 사용하여 셀 프로세스의 프로세스 ID를 제공할 수 있습니다. 셀의 프로세스 ID를 찾으려면 다음과 같은 명령을 사용하십시오.

```
cat /var/run/vmware-vcd-cell.pid
```

command

`cell-application` 하위 명령입니다.

표 5-3. 셀 관리 도구 옵션과 인수, `cell-application` 하위 명령

명령	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--application-states</code>	없음	셀 애플리케이션 및 해당 애플리케이션의 현재 상태를 나열합니다.
<code>--disable</code>	애플리케이션 ID	셀 시작 시 이 셀 애플리케이션이 실행되지 않도록 합니다.
<code>--enable</code>	애플리케이션 ID	셀 시작 시 이 셀 애플리케이션이 실행되도록 합니다.
<code>--pid (-i)</code>	셀 프로세스의 프로세스 ID	<code>-u</code> 또는 <code>-u</code> 와 <code>-p</code> 대신 이 옵션을 사용할 수 있습니다.
<code>--list</code>	없음	모든 셀 애플리케이션을 나열하고 해당 애플리케이션이 셀 시작 시 실행되도록 설정되었는지 표시합니다.

표 5-3. 셀 관리 도구 옵션과 인수, cell-application 하위 명령 (계속)

명령	인수	설명
--password (-p)	VMware Cloud Director 관리자 암호	선택 사항입니다. 암호를 명령줄에 지정하지 않으면 암호를 묻는 메시지가 표시됩니다.
--set	세미콜론으로 구분된 애플리케이션 ID 목록	셀 시작 시 실행되는 셀 애플리케이션 집합을 지정합니다. 이 명령은 셀 시작 시 시작되는 셀 애플리케이션의 기존 집합을 덮어씁니다. 단일 애플리케이션의 시작 상태를 변경하려면 --enable 또는 --disable을 사용합니다.
--username (-u)	VMware Cloud Director 관리자 이름.	--pid를 지정하지 않을 경우 필수 항목입니다.

예제: 셀 애플리케이션 및 해당 애플리케이션의 시작 상태 나열

다음 cell-management-tool 명령줄을 실행하려면 시스템 관리자 자격 증명이 필요하며 이 명령줄은 셀 애플리케이션 목록 및 해당 애플리케이션의 시작 상태를 반환합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool -u administrator cell-application --list
Please enter the administrator password:

name            id            enabled
description

Networking       com.vmware.vc... true         Exposes NSX api endpoints directly from
vCD.
Console Proxy    com.vmware.vc... true         Proxies VM console data
connection...
Cloud Proxy      com.vmware.vc... true         Proxies TCP connections from a tenant
site.
Compute Service Broker com.vmware.vc... true         Allows registering with a service
control...
Maintenance Application com.vmware.vc... false        Indicates to users the cell is
undergo ...
Core Cell Application com.vmware.vc... true         Main cell application, Flex UI and REST
API.
```

데이터베이스 연결 속성 업데이트

셀 관리 도구의 reconfigure-database 하위 명령을 사용하여 VMware Cloud Director 데이터베이스의 연결 속성을 업데이트할 수 있습니다.

VMware Cloud Director 설치 또는 VMware Cloud Director 장치 배포 프로세스 중에 데이터베이스 유형 및 데이터베이스 연결 속성을 구성합니다. [Linux에 VMware Cloud Director 설치 및 VMware Cloud Director 장치의 배포 및 초기 구성](#) 항목을 참조하십시오.

VMware Cloud Director 데이터베이스를 구성한 후에는 `reconfigure-database` 하위 명령을 사용하여 데이터베이스 연결을 업데이트할 수 있습니다. 기존 VMware Cloud Director 데이터베이스를 새 호스트로 이동하거나, 데이터베이스 사용자 이름과 암호를 변경하거나, PostgreSQL 데이터베이스에 대한 SSL 연결을 사용하도록 설정할 수 있습니다.

```
cell-management-tool reconfigure-database options
```

중요 `reconfigure-database` 명령을 실행하여 변경한 내용은 글로벌 구성 파일

`global.properties` 및 셀의 응답 파일 `responses.properties`에 기록됩니다. 명령을 실행하기 전에 응답 파일이 `/opt/vmware/vcloud-director/etc/responses.properties`에 있고 쓰기가 가능한지 확인합니다. 응답 파일 보호 및 재사용에 대한 자세한 내용은 [Linux에 VMware Cloud Director 설치](#)의 내용을 참조하십시오.

--pid 옵션을 사용하지 않는 경우에는 셀을 다시 시작하여 변경 내용을 적용해야 합니다.

표 5-4. 셀 관리 도구 옵션과 인수, reconfigure-database 하위 명령

옵션	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 옵션에 대한 요약을 보여 줍니다.
--database-host (-dbhost)	VMware Cloud Director 데이터베이스 호스트의 IP 주소 또는 FQDN(정규화된 도메인 이름)	database.jdbcUrl 속성의 값을 업데이트합니다. 중요 이 명령은 값 형식만 검증합니다.
--database-instance (-dbinstance)	SQL Server 데이터베이스 인스턴스.	선택 사항입니다. 데이터베이스 유형이 sqlserver인 경우 사용됩니다. 중요 이 옵션을 포함하는 경우 처음에 데이터베이스를 구성할 때 지정한 것과 동일한 값을 제공해야 합니다.
--database-name (-dbname)	데이터베이스 서비스 이름.	database.jdbcUrl 속성의 값을 업데이트합니다.
--database-password (-dbpassword)	데이터베이스 사용자의 암호.	database.password 속성의 값을 업데이트합니다. 제공하는 암호는 속성 값으로 저장되기 전에 암호화됩니다.
--database-port (-dbport)	데이터베이스 호스트의 데이터베이스 서비스에 사용하는 포트 번호.	database.jdbcUrl 속성의 값을 업데이트합니다. 중요 이 명령은 값 형식만 검증합니다.
--database-type (-dbtype)	데이터베이스 유형. 다음 중 하나: ■ sqlserver ■ postgres	database.jdbcUrl 속성의 값을 업데이트합니다.

표 5-4. 셀 관리 도구 옵션과 인수, reconfigure-database 하위 명령 (계속)

옵션	인수	설명
--database-user (-dbuser)	데이터베이스 사용자의 사용자 이름.	database.user 속성의 값을 업데이트합니다.
--database-ssl	true 또는 false	데이터베이스 유형이 postgres인 경우 사용됩니다. VMware Cloud Director에서 SSL 연결을 요구하도록 PostgreSQL 데이터베이스를 구성합니다.
--pid (-i)	셀의 프로세스 ID입니다.	선택 사항입니다. 실행 중인 VMware Cloud Director 셀에서 핫 재구성을 실행합니다. 셀을 다시 시작할 필요가 없습니다. --private-key-path와 함께 사용하면 로컬 및 원격 셀에서 명령을 즉시 실행할 수 있습니다.
--private-key-path	셀의 개인 키 경로 이름.	선택 사항입니다. 서버 그룹의 모든 셀이 정상적으로 종료되고 데이터베이스 속성이 업데이트되고 다시 시작됩니다. 중요 모든 셀은 슈퍼유저의 SSH 연결을 암호 없이 허용해야 합니다.
--remote-sudo-user	sudo 권한이 있는 사용자 이름입니다.	원격 사용자가 루트가 아닌 경우 --private-key-path 옵션과 함께 사용됩니다. 장치의 경우 postgres 사용자에게 이 옵션을 사용할 수 있습니다(예: --remote-sudo-user=postgres).

--database-host 및 --database-port 옵션을 사용하면 명령이 인수의 형식을 확인하지만 호스트와 포트의 조합이 네트워크에 액세스할 수 있는지 또는 지정된 유형의 실행 중인 데이터베이스가 있는지를 테스트하지 않습니다.

--private-key-path 옵션을 사용하는 경우 모든 셀은 슈퍼유저의 SSH 연결을 암호 없이 허용하도록 구성되어야 합니다. 예를 들어 확인을 수행하려면 다음 Linux 명령을 실행할 수 있습니다.

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

이 예제에서는 ID를 vcloud로 설정한 다음 *cell-ip*에 있는 셀에 루트로 SSH 연결을 설정하지만 루트 암호는 제공하지 않습니다. 로컬 셀의 *private-key-path*에 있는 개인 키를 vcloud.vcloud 사용자가 읽을 수 있고, 해당하는 공용 키가 *cell-ip*에서 루트 사용자의 *authorized-keys*에 있으면 명령이 성공합니다.

참고 VMware Cloud Director 프로세스가 실행되는 ID로 사용할 vcloud 사용자, vcloud 그룹 및 vcloud.vcloud 계정이 VMware Cloud Director 설치 관리자에 의해 생성됩니다. vcloud 사용자는 암호가 없습니다.

예제: VMware Cloud Director 데이터베이스 사용자 이름 및 암호 변경

다른 모든 연결 속성을 원래 구성한 상태로 두고 VMware Cloud Director 데이터베이스 사용자 이름과 암호를 변경하려면 다음 명령을 실행합니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \
-dbuser vcd-dba -dbpassword P@55w0rd
```

예제: 모든 셀의 핫 재구성을 통해 VMware Cloud Director 데이터베이스 IP 주소 업데이트

루트가 아닌 사용자이며 sudo 권한이 있는 경우, 모든 셀에서 VMware Cloud Director 데이터베이스의 IP 주소를 즉시 변경하려면 다음 명령을 실행하면 됩니다.

```
[sudo@cell11 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \
--dbhost db_ip_address -i $(service vmware-vcd pid cell) --private-key-path=path_to_private-
key \
--remote-sudo-user=non-root-user
```

손상된 스케줄러 데이터 검색 및 복구

VMware Cloud Director는 Quartz 작업 스케줄러를 사용하여 시스템에서 실행 중인 비동기 작업을 조정합니다. Quartz 스케줄러 데이터베이스가 손상되면 시스템을 정지하지 못할 수 있습니다. 셀 관리 도구의 *fix-scheduler-data* 명령을 사용하여 데이터베이스에서 손상된 스케줄러 데이터를 검색하고 필요한 경우 해당 데이터를 복구할 수 있습니다.

데이터베이스에서 손상된 스케줄러 데이터를 검색하려면 다음 형식의 명령줄을 사용하십시오.

```
cell-management-toolfix-scheduler-dataoptions
```

표 5-5. 셀 관리 도구 옵션과 인수, fix-scheduler-data 하위 명령

옵션	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
--dbuser	VMware Cloud Director 데이터베이스 사용자의 사용자 이름입니다.	명령줄에 제공해야 합니다.
--dbpassword	VMware Cloud Director 데이터베이스 사용자의 암호입니다.	제공하지 않는 경우 암호를 묻는 메시지가 표시됩니다.

HTTPS 및 콘솔 프록시 끝점에 대한 자체 서명된 인증서 생성

셀 관리 도구의 generate-certs 명령을 사용하여 HTTPS 및 콘솔 프록시 끝점에 대한 자체 서명된 SSL 인증서를 생성합니다.

각 VMware Cloud Director 서버 그룹은 두 개의 SSL 끝점을 지원해야 합니다. 하나는 HTTPS 서비스용이고, 다른 하나는 콘솔 프록시 서비스용입니다. HTTPS 서비스 끝점은 VMware Cloud Director Service Provider Admin Portal, VMware Cloud Director Tenant Portal 및 VMware Cloud Director API를 지원합니다. 원격 콘솔 프록시 끝점은 vApp 및 VM에 대한 VMRC 연결을 지원합니다.

셀 관리 도구의 generate-certs 명령은 [Linux에 VMware Cloud Director에 대한 자체 서명된 SSL 인증서 생성 절차를 자동화합니다.](#)

자체 서명된 SSL 인증서를 새로 생성하여 새 keystore나 기존 keystore에 추가하려면 명령줄에 다음과 같은 형식으로 명령을 입력하십시오.

```
cell-management-tool generate-certs options
```

표 5-6. 셀 관리 도구 옵션과 인수, generate-certs 하위 명령

옵션	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
--expiration (-x)	days-until-expiration	인증서 만료일까지 남은 일 수이며, 기본값은 365입니다.
--issuer (-i)	name=value [, name=value, ...]	인증서 발급자의 X.509 고유 이름입니다. 기본값은 CN=FQDN입니다. 여기서 FQDN은 셀의 정규화된 도메인 이름이거나, 정규화된 도메인 이름이 제공되지 않은 경우 셀의 IP 주소입니다. 여러 특성 및 값 쌍을 지정한 경우 쉼표로 구분하고 전체 인수를 따옴표로 묶으십시오.
--httpcert (-j)	없음	HTTPS 끝점에 대한 인증서를 생성합니다.

표 5-6. 셀 관리 도구 옵션과 인수, generate-certs 하위 명령 (계속)

옵션	인수	설명
--type (-t)	<i>keystore-type</i>	키 저장소의 형식입니다. 기본값은 PKCS12입니다. JCEKS 키 저장소를 만들 수도 있습니다.
--key-size (-s)	<i>key-size</i>	비트 단위의 정수로 표현되는 키 쌍의 크기입니다. 기본값은 2048입니다. 1,024보다 작은 키 크기는 NIST Special Publication 800-131A에 따라 더 이상 지원되지 않습니다.
--keystore-pwd (-w)	<i>keystore-password</i>	이 호스트에 있는 keystore의 암호입니다.
--out (-o)	<i>keystore-pathname</i>	이 호스트에 있는 keystore의 전체 경로 이름입니다.
--consoleproxycert (-p)	없음	콘솔 프록시 끝에 대한 인증서를 생성합니다.

참고 이 하위 명령의 이전 릴리스와 호환성을 유지하기 위해 -j 및 -p를 둘 다 생략해도 -j 및 -p를 둘 다 제공한 것과 동일한 결과가 나타납니다.

예제: 자체 서명된 인증서 만들기

두 예제 모두에서 keystore의 위치는 /tmp/cell.ks이고 암호는 kspw라고 가정합니다. 이 keystore는 아직 없는 경우 자동으로 만들어집니다.

이 예제에서는 기본값을 사용하여 새 인증서를 만듭니다. 발급자 이름은 CN=Unknown으로 설정되어 있습니다. 인증서는 기본 2048비트 키 길이를 사용하고, 만든 지 1년 후에 만료됩니다.

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool generate-certs -j -p -o /tmp/cell.ks -w kspw
New keystore created and written to /tmp/cell.ks.
```

이 예제에서는 HTTPS 끝에 대해서만 새 인증서를 만듭니다. 또한 키 크기와 발급자 이름에 대한 사용자 지정 값도 지정합니다. 발급자 이름은 CN=Test, L=London, C=GB로 설정되어 있습니다. HTTPS 연결의 새 인증서는 4096비트 키를 보유하고, 만든 날짜로부터 90일 후에 만료됩니다. 콘솔 프록시 끝에 대한 기존 인증서는 영향을 받지 않습니다.

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool generate-certs -j -o /tmp/cell.ks -w kspw -i "CN=Test, L=London,
C=GB" -s 4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

중요 keystore 파일과 이 파일이 저장된 디렉터리를 vcloud.vcloud 사용자가 읽을 수 있어야 합니다. VMware Cloud Director 설치 관리자가 이 사용자와 그룹을 만듭니다.

HTTPS 및 콘솔 프록시 끝점에 대한 인증서 바꾸기

셀 관리 도구의 `certificates` 명령을 사용하여 HTTPS 및 콘솔 프록시 끝점에 대한 SSL 인증서를 바꿉니다.

셀 관리 도구의 `certificates` 명령은 기존 인증서를 PKCS12 또는 JCEKS 형식 키 저장소에 저장된 새 인증서로 바꾸는 프로세스를 자동화합니다. 자체 서명된 인증서를 서명된 인증서로 바꾸거나 만료되는 인증서를 새 인증서로 바꾸려는 경우 `certificates` 명령을 사용합니다. 서명된 인증서를 포함하는 키 저장소를 만들려면 [Linux에 VMware Cloud Director에 대한 자체 서명된 SSL 인증서 생성 항목을 참조하십시오.](#)

끝점 하나 또는 둘 모두에 대한 SSL 인증서를 바꾸려면 다음과 같은 형식으로 명령을 사용합니다.

```
cell-management-tool certificates options
```

표 5-7. 셀 관리 도구 옵션과 인수, `certificates` 하위 명령

옵션	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--config (-C)</code>	셀의 <code>global.properties</code> 파일에 대한 전체 경로 이름입니다.	기본값은 <code>\$VCLLOUD_HOME/etc/global.properties</code> 입니다.
<code>--https (-j)</code>	없음	http 끝점에서 사용하는 <code>certificates</code> 라는 이름의 <code>keystore</code> 파일을 바꿉니다.
<code>--consoleproxyks (-p)</code>	없음	콘솔 프록시 끝점에서 사용하는 <code>proxycertificates</code> 라는 이름의 <code>keystore</code> 파일을 바꿉니다.
<code>--responses (-r)</code>	셀의 <code>responses.properties</code> 파일에 대한 전체 경로 이름입니다.	기본값은 <code>\$VCLLOUD_HOME/etc/responses.properties</code> 입니다.
<code>--keystore (-k)</code>	<i>keystore-pathname</i>	서명된 인증서가 들어 있는 PKCS12 또는 JCEKS 형식 키 저장소의 전체 경로 이름입니다. 사용되지 않는 <code>-s</code> 짧은 형식이 <code>-k</code> 로 대체되었습니다.
<code>--keystore-password (-w)</code>	<i>keystore-password</i>	<code>--keystore</code> 옵션에서 참조하는 PKCS12 또는 JCEKS 형식 키 저장소의 암호입니다. 사용되지 않는 <code>-kspassword</code> 및 <code>--keystorepwd</code> 옵션을 대체합니다.

예제: 인증서 바꾸기

해당 파일을 기본 위치에서 이동하지 않은 경우 `--config` 및 `--responses` 옵션을 생략할 수 있습니다. 이 예제에서는 `/tmp/my-new-certs.ks`의 `keystore`에 `kspw` 암호가 있습니다. 이 예제에서는 셀의 기존 `http` 끝점 인증서를 `/tmp/my-new-certs.ks`에 있는 인증서로 바꿉니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool certificates -j -k /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

참고 인증서를 바꾼 후에는 셀을 다시 시작해야 합니다.

외부 서비스에서 SSL 인증서 가져오기

셀 관리 도구의 `import-trusted-certificates` 명령을 사용하여 AMQP 및 VMware Cloud Director 데이터베이스와 같은 외부 서비스에 대한 보안 연결 설정에 사용할 인증서를 가져옵니다.

외부 서비스에 대한 보안 연결을 생성하려면 VMware Cloud Director가 서비스의 인증서를 자체 `truststore`로 가져와서 해당 서비스에 대한 유효한 신뢰 체인을 설정해야 합니다. 신뢰할 수 있는 인증서를 셀의 `truststore`로 가져오려면 다음과 같은 형식으로 명령을 사용합니다.

```
cell-management-tool import-trusted-certificates options
```

표 5-8. 셀 관리 도구 옵션과 인수, `import-trusted-certificates` 하위 명령

옵션	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--destination</code>	경로 이름	대상 <code>truststore</code> 에 대한 전체 경로 이름입니다. 명령줄에 제공되지 않은 경우 기본적으로 <code>/opt/vmware/vcloud-director/etc/certificates</code> 로 설정됩니다.
<code>--destination-password</code>	문자열	대상 <code>truststore</code> 에 대한 암호입니다. 명령줄에 제공되지 않은 경우 기본적으로 <code>vcloud.ssl.truststore.password</code> 의 값으로 설정됩니다.
<code>--destination-type</code>	키 저장소 유형	대상 <code>truststore</code> 의 키 저장소 유형입니다. JKS 또는 JCEKS일 수 있습니다. 기본적으로 JCEKS로 설정됩니다.

표 5-8. 셀 관리 도구 옵션과 인수, import-trusted-certificates 하위 명령 (계속)

옵션	인수	설명
--force	없음	대상 truststore의 기존 인증서를 덮어 씁니다.
--source	경로 이름	소스 PEM 파일에 대한 전체 경로 이름입니다.

예제: 신뢰할 수 있는 인증서 가져오기

이 예제에서는 인증서를 /tmp/demo.pem에서 /opt/vmware/vcloud-director/etc/certificates의 VMware Cloud Director 로컬 키 저장소로 가져옵니다. VMware Cloud Director는 키 저장소 암호를 암호화된 형식으로 저장하며, 이 암호는 import-trusted-certificates 명령으로 해독합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem
```

vSphere 리소스에서 끝점 인증서 가져오기

업그레이드 후 셀 관리 도구의 trust-infra-certs 명령을 사용하여 환경의 vSphere 리소스에서 VMware Cloud Director 데이터베이스로 인증서를 수집하고 가져옵니다.

셀 관리 도구의 trust-infra-certs 명령은 환경의 vSphere 리소스에서 SSL 인증서를 자동으로 수집하여 VMware Cloud Director 데이터베이스로 가져옵니다.

사전 요구 사항

끝점을 가져올 vCenter Server 및 NSX Manager 인스턴스가 가동되어 실행 중인지 확인합니다.

절차

- 1 VMware Cloud Director 셀의 OS에 root로 로그인하거나 SSH를 통해 연결합니다.
- 2 다음 형식으로 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs options
```

표 5-9. 셀 관리 도구 옵션과 인수, trust-infra-certs 하위 명령

옵션	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약물을 보여 줍니다.
--vsphere	없음	이 설치에서 등록된 모든 vCenter Server, NSX Data Center for vSphere 및 NSX-T Data Center 인스턴스에 대한 인증서를 신뢰하라는 메시지를 표시합니다.

표 5-9. 셀 관리 도구 옵션과 인수, trust-infra-certs 하위 명령 (계속)

옵션	인수	설명
--trust	없음	선택 사항입니다. VMware Cloud Director truststore에 인증서를 추가합니다.
--inspect	선택 사항입니다. 파일 경로.	선택 사항입니다. 인증서를 파일로 표시합니다.
--unattended	없음	선택 사항입니다. 이 옵션과 함께 호출되면 명령에서 추가 입력을 요청하지 않습니다. 모든 인프라 인증서가 자동으로 신뢰됩니다.

예제: vSphere 리소스 끝점에서 모든 인증서 신뢰 및 가져오기

추가 입력을 요구하지 않고 vSphere 리소스 끝점에서 인증서를 신뢰하고 가져오려면 다음 옵션을 사용하여 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs --vsphere --unattended
```

테스트 연결 거부 목록 구성

설치 또는 업그레이드 후에는 VMware Cloud Director 네트워크에 대한 액세스 권한을 테넌트에게 제공하기 전에 먼저 셀 관리 도구의 manage-test-connection-blacklist 명령을 사용하여 내부 호스트에 대한 액세스를 차단합니다.

VMware Cloud Director 10.1부터 서비스 제공자 및 테넌트가 VMware Cloud Director API를 사용하여 원격 서버에 대한 연결을 테스트하고 SSL 핸드셰이크의 일부로 서버 ID를 확인할 수 있습니다.

악의적인 공격으로부터 VMware Cloud Director 인스턴스가 배포된 내부 네트워크를 보호하기 위해 시스템 제공자는 테넌트가 연결할 수 없는 내부 호스트의 거부 목록을 구성할 수 있습니다.

이렇게 하면 테넌트 액세스 권한이 있는 악의적인 공격자가 연결 테스트 VMware Cloud Director API를 사용하여 VMware Cloud Director가 설치된 네트워크를 매핑하려고 하면 거부 목록에 있는 내부 호스트에 연결할 수 없습니다.

설치 또는 업그레이드 후 VMware Cloud Director 네트워크에 대한 액세스 권한을 테넌트에게 제공하기 전에 셀 관리 도구의 manage-test-connection-blacklist 명령을 사용하여 내부 호스트에 대한 테넌트 연결을 차단합니다.

절차

- 1 VMware Cloud Director 셀의 OS에 root로 로그인하거나 SSH를 통해 연결합니다.
- 2 다음 명령을 실행하여 거부 목록에 항목을 추가합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-test-connection-blacklist option
```

표 5-10. 셀 관리 도구 옵션과 인수, manage-test-connection-blacklist 하위 명령

옵션	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
--add-ip	IPv4 또는 IPv6 주소	거부 목록에 IP 주소를 추가합니다.
--add-name	호스트에 대한 하위 도메인 또는 정규화된 도메인 이름	거부 목록에 하위 도메인 또는 도메인 이름을 추가합니다.
--add-range	CIDR 또는 하이픈 형식의 IPv4 또는 IPv6 주소 범위	거부 목록에 IP 주소 범위를 추가합니다.
--list	없음	액세스가 거부된 기존 항목을 모두 나열합니다.

모든 활성 셀의 FIPS 상태 보기

VMware Cloud Director 10.2.2부터 모든 활성 VMware Cloud Director 셀의 FIPS 상태를 확인하기 위해 `fips-status` 명령을 사용할 수 있습니다. 이 명령은 VMware Cloud Director 장치의 FIPS 상태를 표시하지 않습니다.

Linux에서 VMware Cloud Director에 대해 FIPS 모드를 사용하도록 설정하는 방법에 대한 자세한 내용은 "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 [FIPS 모드 사용](#)을 참조하십시오.

`fips-status` 명령은 모든 활성 셀에 대한 FIPS 상태 정보(예: 셀 이름, UUID, IP주소 및 FIPS 상태)를 표시합니다.

장치 FIPS 모드 정보에 대한 자세한 내용은 [VMware Cloud Director 장치 FIPS 모드 보기](#)에서 참조하십시오.

JSON 형식의 데이터를 수신하려면 `--json` 플래그를 지정하면 됩니다.

절차

- 1 VMware Cloud Director 셀의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 모든 활성 셀의 FIPS 상태를 봅니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool fips-status
```

표 5-11. 셀 관리 도구 옵션과 인수, fips-status 명령

명령	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
--json	없음	정보를 JSON 형식으로 표시합니다.

허용되는 SSL 암호화 목록 관리

셀 관리 도구의 `ciphers` 명령을 사용하여 SSL 핸드셰이크 프로세스 도중 사용하기 위해 셀이 제공하는 암호화 스위트 집합을 구성합니다.

참고 `ciphers` 명령은 VMware Cloud Director 장치가 해당 장치 관리 사용자 인터페이스 및 API에 사용하는 인증서가 아니라 VMware Cloud Director가 HTTPS 및 콘솔 프록시 통신에 사용하는 인증서 집합에만 적용됩니다.

클라이언트가 VMware Cloud Director 셀에 대한 SSL 연결을 만들면, 셀은 허용 암호화 기본 목록에 구성되어 있는 암호화만 사용하도록 제공합니다. 연결의 보안을 유지할 수 있을 만큼 충분히 강력하지 않거나 SSL 연결 실패에 관련된 것으로 알려진 일부 암호화는 이 목록에 나열되지 않습니다.

VMware Cloud Director를 설치하거나 업그레이드할 경우 설치 또는 업그레이드 스크립트를 통해 셀의 인증서가 검사됩니다. 허용된 암호 목록에 없는 암호를 사용하여 암호화된 인증서가 있으면 설치 또는 업그레이드가 실패합니다. 다음 단계를 수행하여 인증서를 교체하고 허용된 암호 목록을 재구성할 수 있습니다.

- 1 허용되지 않는 암호를 사용하지 않는 인증서를 만듭니다. 아래 예제에 나와 있는 것처럼 `cell-management-tool ciphers -a`를 사용하여 기본 구성에서 허용되는 모든 암호화를 나열할 수 있습니다.
- 2 `cell-management-tool certificates` 명령을 사용하여 셀의 기존 인증서를 새 인증서로 바꿉니다.
- 3 `cell-management-tool ciphers` 명령을 사용하여 허용된 암호 목록을 재구성하고 새 인증서와 함께 사용하는 데 필요한 모든 암호를 포함합니다.

중요 VMRC 콘솔에서는 AES256-SHA 및 AES128-SHA 암호화를 사용해야 하기 때문에 VMware Cloud Director 클라이언트에서 VMRC 콘솔을 사용할 경우 AES256-SHA 및 AES128-SHA 암호화를 허용해야 합니다.

허용 SSL 암호화 목록을 관리하려면 다음 형식의 명령줄을 사용하십시오.

```
cell-management-tool ciphers options
```

표 5-12. 셀 관리 도구 옵션과 인수, `ciphers` 하위 명령

옵션	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--all-allowed (-a)</code>	없음	VMware Cloud Director가 지원하는 모든 암호를 나열합니다.
<code>--compatible-reset (-c)</code> (폐기됨)	없음	더 이상 사용되지 않습니다. 허용된 암호의 기본 목록으로 재설정하려면 <code>--reset</code> 옵션을 사용합니다.

표 5-12. 셀 관리 도구 옵션과 인수, ciphers 하위 명령 (계속)

옵션	인수	설명
<code>--disallow (-d)</code>	선택으로 구분된 암호화 이름 목록입니다.	<p>지정된 목록(선택으로 구분된 목록)의 암호화를 허용하지 않습니다. 이 옵션을 실행할 때마다 비활성화하려는 전체 암호화 목록을 포함해야 합니다. 옵션을 실행하면 이전 설정을 덮어쓰기 때문입니다.</p> <p>중요 값 없이 옵션을 실행하면 모든 암호가 활성화됩니다.</p> <p>가능한 모든 암호를 보려면 <code>-a</code> 옵션을 실행합니다.</p> <p>중요 <code>ciphers --disallow</code>를 실행한 후 셀을 다시 시작해야 합니다.</p>
<code>--list (-l)</code>	없음	현재 사용 중인 허용된 암호 집합을 나열합니다.
<code>--reset (-r)</code>	없음	<p>허용된 암호의 기본 목록으로 재설정합니다. 이 셀의 인증서에 허용되지 않는 암호를 사용할 경우, 허용된 암호를 사용하는 새 인증서를 설치할 때까지 셀에 SSL 연결을 설정할 수 없습니다.</p> <p>중요 <code>ciphers --reset</code>를 실행한 후 셀을 다시 시작해야 합니다.</p>

예제: 2개 암호화를 허용 안 함

VMware Cloud Director에는 사용하도록 설정된 암호의 미리 구성된 목록이 포함되어 있습니다.

이 예에서는 허용된 암호 목록에서 추가 암호를 사용하도록 설정하는 방법과 사용하지 않으려는 암호를 허용하지 않는 방법을 설명합니다.

- 1 기본적으로 사용하도록 설정된 암호 목록을 가져옵니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -l
```

명령의 출력은 사용하도록 설정된 암호 목록을 반환합니다.

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

2 SSL 핸드셰이크 중에 셀이 제공할 수 있는 모든 암호 목록을 가져옵니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
```

명령의 출력은 허용된 암호 목록을 반환합니다.

```
# ./cell-management-tool ciphers -a
Product default ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
```

3 비활성화할 암호를 지정합니다.

명령을 실행하며 암호를 명시적으로 비활성화하지 않으면 해당 암호는 활성화됩니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool ciphers -d
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
```

4 명령을 실행하여 활성화된 암호 목록을 확인합니다. 목록에 없는 암호는 비활성화됩니다.

```
root@bos1-vcd-static-211-90 [ /opt/vmware/vcloud-
director/bin ]# ./cell-management-tool ciphers -l
```

이제 사용하도록 설정된 모든 암호 목록이 출력에 반환됩니다.

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

```
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
```

허용되는 SSL 프로토콜 목록 관리

SSL 핸드셰이크 프로세스 중에 사용하도록 셀이 제공하는 SSL 프로토콜 집합을 구성하려면 셀 관리 도구의 `ssl-protocols` 명령을 사용합니다.

클라이언트가 VMware Cloud Director 셀에 대한 SSL 연결을 만들면, 셀은 허용된 SSL 프로토콜 목록에 구성되어 있는 프로토콜만 사용하도록 제공합니다. TLSv1, SSLv3 및 SSLv2Hello를 포함한 몇 가지 프로토콜은 심각한 보안 취약점이 있는 것으로 알려졌기 때문에 기본 목록에 포함되어 있지 않습니다.

절차

- 1 VMware Cloud Director 셀의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 허용되는 SSL 프로토콜 목록을 관리하는 명령을 실행합니다.

```
cell-management-tool ssl-protocols options
```

표 5-13. 셀 관리 도구 옵션과 인수, `ssl-protocols` 하위 명령

옵션	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--all-allowed (-a)</code>	없음	VMware Cloud Director가 지원하는 모든 SSL 프로토콜을 나열합니다.

표 5-13. 셀 관리 도구 옵션과 인수, `ssl-protocols` 하위 명령 (계속)

옵션	인수	설명
<code>--disallow (-d)</code>	선택으로 구분된 SSL 프로토콜 이름의 목록입니다.	<p>허용되지 않는 SSL 프로토콜의 목록을 목록에 지정된 프로토콜로 재구성합니다. 이 옵션을 실행할 때마다 비활성화하려는 SSL 프로토콜의 전체 목록을 포함해야 합니다. 옵션을 실행하면 이전 설정을 덮어쓰기 때문입니다.</p> <p>중요 값 없이 옵션을 실행하면 모든 SSL 프로토콜이 활성화됩니다.</p> <p>가능한 모든 SSL 프로토콜을 보려면 <code>-a</code> 옵션을 실행합니다.</p> <p>중요 <code>ssl-protocols --disallow</code>를 실행한 후 셀을 다시 시작해야 합니다.</p>
<code>--list (-l)</code>	없음	현재 사용 중인 허용된 SSL 프로토콜 집합을 나열합니다.
<code>--reset (-r)</code>	없음	구성된 SSL 프로토콜의 목록을 공장 기본값으로 재설정합니다.
		<p>중요 <code>ssl-protocols --reset</code>을 실행한 후 셀을 다시 시작해야 합니다.</p>

예제: 허용 및 구성된 SSL 프로토콜 나열 및 허용되지 않는 SSL 프로토콜 목록 재구성

SSL 핸드셰이크 도중 셀이 제공할 수 있는 모든 SSL 프로토콜을 나열하려면 `--all-allowed(-a)` 옵션을 사용합니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

* TLSv1.2
* TLSv1.1
* TLSv1
* SSLv3
* SSLv2Hello
```

이 목록은 일반적으로 셀이 지원하도록 구성된 SSL 프로토콜의 상위 집합입니다. 해당 SSL 프로토콜을 나열하려면 `--list (-l)` 옵션을 사용하십시오.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:
```

```
* TLSv1.2
* TLSv1.1
```

허용되지 않는 SSL 프로토콜 목록을 재구성하려면 `--disallow(-d)` 옵션을 사용합니다. 이 옵션에는 `ssl-protocols -a`에 의해 생성된 쉘표로 구분된 허용 프로토콜의 하위 집합 목록이 필요합니다.

이 예에서는 TLSv1을 포함하도록 허용되는 SSL 프로토콜 목록을 업데이트합니다. 5.5 업데이트 3e 이전의 vCenter Server 릴리스에는 TLSv1이 필요합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool ssl-protocols -d SSLv3,SSLv2Hello
```

이 명령을 실행한 후에는 셀을 다시 시작해야 합니다.

메트릭 수집 및 게시 구성

셀 관리 도구의 `configure-metrics` 명령을 사용하여 수집할 메트릭 집합을 구성할 수 있습니다.

VMware Cloud Director는 가상 시스템 성능 및 리소스 사용에 대한 현재 및 이전 정보를 제공하는 메트릭을 수집할 수 있습니다. VMware Cloud Director가 수집하는 메트릭을 구성하려면 이 하위 명령을 사용합니다. VMware Cloud Director 메트릭 저장소로 사용하기 위해 Apache Cassandra 데이터베이스를 구성하려면 `cell-management-toolcassandra` 하위 명령을 사용합니다. [Cassandra 메트릭 데이터베이스 구성](#)의 내용을 참조하십시오.

절차

- 1 VMware Cloud Director 셀의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 VMware Cloud Director가 수집하는 메트릭을 구성합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool configure-metrics --metrics-config
pathname
```

표 5-14. 셀 관리 도구 옵션과 인수, `configure-metrics` 하위 명령

명령	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--repository-host(사용되지 않음)</code>	KairosDB 호스트의 호스트 이름 또는 IP 주소	더 이상 사용되지 않습니다. VMware Cloud Director 메트릭 저장소로 사용하기 위해 Apache Cassandra 데이터베이스를 구성하려면 <code>cell-management-toolcassandra</code> 하위 명령의 <code>--cluster-nodes</code> 옵션을 사용합니다.

표 5-14. 셀 관리 도구 옵션과 인수, configure-metrics 하위 명령 (계속)

명령	인수	설명
--repository-port(사용되지 않음)	사용할 KairosDB 포트입니다.	더 이상 사용되지 않습니다. VMware Cloud Director 메트릭 저장소로 사용하기 위해 Apache Cassandra 데이터베이스를 구성하려면 cell-management-tool cassandra 하위 명령의 --port 옵션을 사용합니다.
--metrics-config	경로 이름	메트릭 구성 파일의 경로

- 3 VMware Cloud Director 버전이 10.2.2 이상인 경우 다음 명령을 실행하여 메트릭 계시를 사용하도록 설정할 수도 있습니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

VMware Cloud Director 10.2.2부터는 메트릭 계시가 기본적으로 비활성화됩니다.

예제: 메트릭 데이터베이스 연결 구성

이 예제에서는 /tmp/metrics.groovy 파일에 지정된 대로 메트릭 수집을 구성합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

VMware Cloud Director 메트릭 수집 서비스는 vSphere Performance Manager가 수집한 메트릭의 하위 집합을 구현합니다. 메트릭 이름과 수집 매개 변수에 대한 자세한 내용은 vSphere Performance Manager 설명서를 참조하십시오. metrics-config 파일에는 하나 이상의 메트릭 이름이 포함되어 있으며 포함된 각 메트릭에 대한 수집 매개 변수를 제공합니다. 예는 다음과 같습니다.

```
configuration {
  metric("cpu.usage.average")
  metric("cpu.usagemhz.average")
  metric("cpu.usage.maximum")
  metric("disk.used.latest") {
    currentInterval=300
    historicInterval=300
    entity="VM"
    instance=""
    minReportingInterval=1800
    aggregator="AVERAGE"
  }
}
```

다음 메트릭 이름이 지원됩니다.

표 5-15. 메트릭 이름

메트릭 이름	설명
cpu.usage.average	총 사용 가능 CPU 중 이 가상 시스템에서 활발히 사용하는 평균 CPU의 비율로 표시되는 호스트 보기. 모든 소켓의 모든 코어가 포함됩니다.
cpu.usagemhz.average	이 가상 시스템에서 활발히 사용하는 평균 CPU 원시 측정값의 호스트 보기. 모든 소켓의 모든 코어가 포함됩니다.
cpu.usage.maximum	총 사용 가능 CPU 중 이 가상 시스템에서 활발히 사용하는 최대 CPU의 비율로 표시되는 호스트 보기. 모든 소켓의 모든 코어가 포함됩니다.
mem.usage.average	구성된 총 메모리 중 이 가상 시스템에서 사용하는 메모리의 비율.
disk.provisioned.latest	포함하는 조직 가상 데이터 센터에서 이 가상 하드 디스크에 할당된 스토리지 공간.
disk.used.latest	모든 가상 하드 디스크에서 사용하는 스토리지.
disk.read.average	모든 가상 하드 디스크에 대한 평균 읽기 속도.
disk.write.average	모든 가상 하드 디스크에 대한 평균 쓰기 속도.

참고 가상 시스템에 여러 개의 디스크가 있는 경우 VMware Cloud Director는 모든 디스크에 대한 집계로 메트릭을 보고합니다. CPU 메트릭은 모든 코어 및 소켓의 집계입니다.

이름이 지정된 각 메트릭에 대해 다음 수집 매개 변수를 지정할 수 있습니다.

표 5-16. 메트릭 수집 매개 변수

매개 변수 이름	값	설명
currentInterval	초(정수)	현재 메트릭 쿼리에 대해 사용 가능한 최신 메트릭 값을 쿼리할 때 사용할 간격(초)입니다. 기본값은 20입니다. vSphere Performance Manager에 정의된 대로 VMware Cloud Director는 수준 1 메트릭에 대해서만 20보다 큰 값을 지원합니다.
historicInterval	초(정수)	기간별 메트릭 값에 대해 쿼리할 때 사용할 초 단위 간격. 기본값은 20입니다. vSphere Performance Manager에 정의된 대로 VMware Cloud Director는 수준 1 메트릭에 대해서만 20보다 큰 값을 지원합니다.
entity	다음 중 하나: HOST, VM	메트릭을 사용할 수 있는 VC 개체의 유형입니다. 기본값은 VM입니다. 모든 엔터티에 대해 모든 메트릭을 사용할 수 있는 것은 아닙니다.
instance	vSphere Performance Manager PerfMetricId 인스턴스 식별자	메트릭의 개별 인스턴스(예: 개별 CPU 코어), 모든 인스턴스의 집계 또는 두 가지 모두에 대한 데이터를 검색할지 여부를 나타냅니다. "*" 값은 모든 메트릭(인스턴스 및 집계)을 수집합니다. 빈 문자열 ""는 집계 데이터만 수집합니다. "DISKFILE"과 같은 특정 문자열은 해당 인스턴스에 대한 데이터만 수집합니다. 기본값은 "*"입니다.

표 5-16. 메트릭 수집 매개 변수 (계속)

매개 변수 이름	값	설명
minReportingInterval	초(정수)	시계열 데이터를 보고할 때 사용할 초 단위 기본 집계 간격을 지정합니다. 수집 간격의 세분성이 충분하지 않은 경우 보고 세분성에 대한 추가적인 제어를 제공합니다. 기본값은 0입니다. 즉, 전용 보고 간격이 없습니다.
aggregator	다음 중 하나: AVERAGE, MINIMUM, MAXIMUM, SUMMATION	minReportingInterval 동안 수행할 집계의 유형. 기본값은 AVERAGE입니다.

Cassandra 메트릭 데이터베이스 구성

셀 관리 도구의 `cassandra` 명령을 사용하여 셀을 메트릭 데이터베이스(선택 사항)에 연결합니다.

VMware Cloud Director는 가상 시스템 성능 및 리소스 사용에 대한 현재 및 이전 정보를 제공하는 메트릭을 수집할 수 있습니다. VMware Cloud Director 메트릭 저장소로 사용하기 위해 **Apache Cassandra** 데이터베이스를 구성하려면 이 하위 명령을 사용합니다. 수집할 메트릭 집합을 구성하려면 도구에 대해 `cell-management-tool configure-metrics` 하위 명령을 사용합니다. **메트릭 수집 및 게시 구성**의 내용을 참조하십시오.

이전 메트릭에 대한 데이터는 **Apache Cassandra** 데이터베이스에 저장됩니다. 성능 메트릭을 저장하고 검색하기 위한 선택적 데이터베이스 소프트웨어 구성에 대한 자세한 내용은 **기간별 메트릭 데이터 저장을 위한 Cassandra 데이터베이스 설치 및 구성** 항목을 참조하십시오.

VMware Cloud Director와 Apache Cassandra 데이터베이스 간에 연결을 생성하려면 다음과 같은 형식으로 명령줄을 사용합니다.

```
cell-management-tool cassandra options
```

표 5-17. 셀 관리 도구 옵션과 인수, `cassandra` 하위 명령

명령	인수	설명
<code>--help (-h)</code>	없음	이 명령에서 사용할 수 있는 옵션에 대한 요약을 보여 줍니다.
<code>--add-rollup</code>	없음	롤업된 메트릭을 포함하도록 메트릭 스키마를 업데이트합니다. 기간별 메트릭 데이터 저장 을 위한 Cassandra 데이터베이스 설치 및 구성 의 내용을 참조하십시오.
<code>--cluster-nodes</code>	<code>address[, address ...]</code>	VMware Cloud Director 메트릭에 사용할 쉼표로 구분된 Cassandra 클러스터 노드 목록입니다.
<code>--clean</code>	없음	VMware Cloud Director 데이터베이스에서 Cassandra 구성 설정을 제거합니다.

표 5-17. 셀 관리 도구 옵션과 인수, cassandra 하위 명령 (계속)

명령	인수	설명
--configure	없음	기존 Cassandra 클러스터와 함께 사용할 VMware Cloud Director를 구성합니다.
--dump	없음	현재 연결 구성을 버립니다.
--keyspace	문자열	Cassandra의 VMware Cloud Director 키 공간 이름을 <i>string</i> 으로 설정합니다. 기본값은 <code>vcloud_metrics</code> 입니다.
--offline	없음	VMware Cloud Director에서 사용할 Cassandra를 구성하지만 VMware Cloud Director에 대한 연결로 구성을 테스트하지 않습니다.
--password	문자열	Cassandra 데이터베이스 사용자의 암호입니다.
--port	정수	각 클러스터 노드에서 연결할 포트입니다. 기본값은 9042입니다.
--ttl	정수	<i>integer</i> 일 동안 메트릭 데이터를 유지합니다. 메트릭 데이터를 영원히 유지하려면 <i>integer</i> 를 0으로 설정합니다.
--update-schema	없음	Cassandra 스키마를 초기화하여 VMware Cloud Director 메트릭 데이터를 저장합니다.
--username	문자열	Cassandra 데이터베이스 사용자의 사용자 이름입니다.

예제: Cassandra 데이터베이스 연결 구성

다음과 같은 명령을 사용합니다. 여기서 *node1-ip*, *node2-ip*, *node3-ip* 및 *node4-ip*는 Cassandra 클러스터 멤버의 IP 주소입니다. 기본 포트(9042)가 사용됩니다. 메트릭 데이터는 15일 동안 유지됩니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --configure --create-schema \ --cluster-nodes node1-
ip,node2-ip,node3-ip, node4-ip \ --username admin --password 'P@55w0rd' --ttl 15
```

이 명령을 완료한 후에는 셀을 다시 시작해야 합니다.

시스템 관리자 암호 복구

VMware Cloud Director 데이터베이스 사용자 이름과 암호를 아는 경우 셀 관리 도구의 `recover-password` 명령을 사용하여 VMware Cloud Director 시스템 관리자 암호를 복구할 수 있습니다.

셀 관리 도구의 `recover-password` 명령을 사용하면 VMware Cloud Director 데이터베이스 사용자 이름과 암호를 아는 사용자가 VMware Cloud Director 시스템 관리자 암호를 복구할 수 있습니다.

시스템 관리자 암호를 복구하려면 명령줄에 다음 형식의 명령을 입력하십시오.

```
cell-management-tool recover-password options
```

표 5-18. 셀 관리 도구 옵션과 인수, `recover-password` 하위 명령

옵션	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--dbuser</code>	VMware Cloud Director 데이터베이스 사용자의 사용자 이름입니다.	명령줄에 제공해야 합니다.
<code>--dbpassword</code>	VMware Cloud Director 데이터베이스 사용자의 암호입니다.	제공하지 않는 경우 암호를 묻는 메시지가 표시됩니다.

작업의 실패 상태 업데이트

셀이 고의로 종료되었을 때 실행 중이던 작업과 연관된 완료 상태를 업데이트하려면 셀 관리 도구의 `fail-tasks` 명령을 사용합니다. `fail-tasks` 명령은 모든 셀이 종료된 경우에만 사용할 수 있습니다.

`cell-management-tool -q` 명령을 사용하여 셀을 정지할 경우 몇 분 내에 실행 중인 작업이 정상적으로 종료되어야 합니다. 중지된 셀에서 작업이 계속 실행되는 경우 슈퍼유저가 셀을 종료할 수 있으며 이 경우 실행 중인 모든 작업이 강제로 실패 처리됩니다. 실행 중인 작업을 강제로 실패 처리하는 종료를 수행한 후 슈퍼유저는 `cell-management-tool fail-tasks`를 실행하여 해당 작업의 완료 상태를 업데이트할 수 있습니다. 작업의 완료 상태를 업데이트하는 이러한 방법은 선택 사항이지만 관리 작업으로 인한 실패를 명확하게 식별하여 시스템 로그의 무결성을 유지하는 데 도움이 됩니다.

중지된 셀에서 아직 실행 중인 작업의 목록을 생성하려면 다음 형식의 명령줄을 사용합니다.

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

표 5-19. 셀 관리 도구 옵션과 인수, `fail-tasks` 하위 명령

명령	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--message (-m)</code>	메시지 텍스트	작업 완료 상태에 배치할 메시지 텍스트입니다.

예제: 셸에서 실행 중인 작업을 실패한 것으로 처리

이 예에서는 셸이 종료될 때 여전히 실행 중이던 작업과 연관된 작업 완료 상태를 업데이트합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool fail-tasks -m "administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system,
Organization: org1
Would you like to fail the tasks listed above?
```

작업을 **관리 종료**의 완료 상태로 업데이트하려면 **y**를 입력합니다. 작업을 계속 실행할 수 있도록 허용하려면 **n**을 입력합니다.

참고 여러 개의 작업이 응답으로 반환된 경우 해당 모든 작업을 실패 처리할지 또는 조치를 취하지 않을지 결정해야 합니다. 작업의 일부만 선택하여 실패 처리할 수 없습니다.

감사 메시지 처리 구성

셸 관리 도구의 `configure-audit-syslog` 명령을 사용하여 시스템이 감사 메시지를 기록하는 방식을 구성합니다.

각 VMware Cloud Director 셸의 서비스는 감사 메시지를 VMware Cloud Director 데이터베이스에 기록합니다. 감사 메시지는 여기서 90일 동안 보존됩니다. 감사 메시지를 더 길게 보존하기 위해 감사 메시지를 VMware Cloud Director 데이터베이스 외에 Linux syslog 유틸리티에 전송하도록 VMware Cloud Director 서비스를 구성할 수 있습니다.

시스템 구성 스크립트를 사용하면 감사 메시지가 처리되는 방식을 지정할 수 있습니다. "VMware Cloud Director 설치, 구성 및 업그레이드 가이드"의 "네트워크 및 데이터베이스 연결 구성"을 참조하십시오. 시스템 구성 중에 지정하는 로깅 옵션은 `global.properties` 및 `responses.properties`의 두 파일에 보존됩니다. 다음 형식의 셸 관리 도구 명령줄을 사용하여 두 파일의 감사 메시지 로깅 구성을 변경할 수 있습니다.

```
cell-management-toolconfigure-audit-syslog options
```

이 셸 관리 도구 하위 명령으로 만들어진 모든 변경 내용은 셸의 `global.properties` 및 `responses.properties` 파일에 보존됩니다. 변경 내용은 셸을 다시 시작할 때까지 적용되지 않습니다.

표 5-20. 셸 관리 도구 옵션과 인수, configure-audit-syslog 하위 명령

옵션	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
--disable (-d)	없음	감사 이벤트를 syslog에 로깅하는 기능을 비활성화합니다. 감사 이벤트는 VMware Cloud Director 데이터베이스에만 로깅합니다. 이 옵션은 global.properties 및 responses.properties에서 audit.syslog.host 및 audit.syslog.port의 값을 설정 취소합니다.
--syslog-host (-loghost)	syslog 서버 호스트의 IP 주소 또는 정규화된 도메인 이름	이 옵션은 audit.syslog.host 속성의 값을 지정된 주소 또는 정규화된 도메인 이름에 설정합니다.
--syslog-port (-logport)	0-65535 사이의 정수	이 옵션은 audit.syslog.port 속성의 값을 지정된 정수에 설정합니다.

--syslog-host, --syslog-port 또는 둘 다에 대해 값을 지정하는 경우 명령은 지정된 값의 형식이 올바른지 확인하지만 실행 중인 syslog 서비스가 있는지 여부 또는 네트워크 액세스에 대한 호스트와 포트의 조합을 테스트하지 않습니다.

예제: Syslog 서버 호스트 이름 변경

중요 이 명령으로 수행된 변경 내용은 글로벌 구성 파일과 지시 파일에 기록됩니다. 이 명령을 사용하기 전에 지시 파일이 /opt/vmware/vcloud-director/etc/responses.properties에 있고 쓰기 가능한지 확인해야 합니다. "VMware Cloud Director 설치, 구성 및 업그레이드 가이드"의 "지시 파일 보호 및 다시 사용"을 참조하십시오.

syslog 메시지가 전송되는 호스트를 변경하려면 다음과 같은 명령을 사용합니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]#
cell-management-tool configure-audit-syslog -loghost syslog.example.com
Using default port 514
```

이 예제에서는 새 호스트가 기본 포트에서 syslog 메시지를 수신한다고 가정합니다.

이 명령은 global.properties 및 responses.properties를 업데이트하지만 셸을 다시 시작할 때까지 변경 내용은 적용되지 않습니다.

e-메일 템플릿 구성

e-메일 경고를 만들 때 시스템에서 사용하는 템플릿을 관리하려면 셀 관리 도구의 `manage-email` 명령을 사용할 수 있습니다.

시스템은 기본적으로 e-메일 경고를 통해 시스템 관리자의 개입이 필요할 수 있는 이벤트와 상태를 시스템 관리자에게 알립니다. e-메일 받는 사람의 목록은 VMware Cloud Director API 또는 웹 콘솔을 사용하여 업데이트할 수 있습니다. 다음 형식의 셀 관리 도구 명령줄을 사용하여 각 종류의 경고에 대한 기본 e-메일 콘텐츠를 재정의할 수 있습니다.

```
cell-management-tool manage-email options
```

표 5-21. 셀 관리 도구 옵션과 인수, `manage-email` 하위 명령

옵션	인수	설명
<code>--help</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--delete</code>	템플릿 이름	삭제할 템플릿의 이름입니다.
<code>--lookup</code>	템플릿 이름	이 인수는 선택 사항입니다. 이 인수를 제공하지 않으면 모든 템플릿 이름의 목록이 반환됩니다.
<code>--locale</code>	템플릿 로케일	기본적으로 이 명령은 <code>en-US</code> 로케일의 템플릿에서 작동합니다. 다른 로케일을 지정하려면 이 옵션을 사용합니다.
<code>--set-template</code>	업데이트된 e-메일 템플릿이 들어 있는 파일에 대한 경로 이름	이 파일은 로컬 호스트에서 액세스할 수 있어야 하며 사용자 <code>vcloud.vcloud</code> 가 읽을 수 있어야 합니다. 예를 들면 <code>/tmp/my-email-template.txt</code> 와 같습니다.

여러 e-메일 알림에 사용할 수 있는 여러 개의 허용된 템플릿 이름이 있습니다.

표 5-22. VMware Cloud Director e-메일 알림 이름

이름	설명	e-메일 전송 시점	받는 사람
<code>VAPP_UNDEPLOY_NOTIFICATION_BODY</code>	vApp의 런타임 임대 만료가 임박했을 때 경고합니다. 임대 만료되면 VMware Cloud Director가 vApp을 일시 중단하거나 전원을 끕니다.	구성된 배포 및 스토리지 임대 경고 시간에 따라 vApp의 런타임 임대가 만료되기 전.	vApp의 소유자가 알림을 받거나 소유자가 시스템 관리자 인 경우 조직 관리자 가 알림을 받습니다.
<code>VAPP_STORAGE_NOTIFICATION_BODY</code>	vApp의 스토리지 임대 만료가 임박했을 때 경고합니다. 임대 만료되면 VMware Cloud Director가 vApp을 삭제합니다.	구성된 배포 및 스토리지 임대 경고 시간에 따라 vApp의 스토리지 임대가 만료되기 전.	vApp의 소유자가 알림을 받거나 소유자가 시스템 관리자 인 경우 조직 관리자 가 알림을 받습니다.

표 5-22. VMware Cloud Director e-메일 알림 이름 (계속)

이름	설명	e-메일 전송 시점	받는 사람
VAPP_STORAGE_NOTIFICATION_FAILED	vApp 스토리지 임대 매트로가 임박했을 때 경고합니다. 임대 매트로가 만료되면 VMware Cloud Director가 vApp을 만료된 것으로 표시합니다.	구성된 배포 및 스토리지 임대 경고 시간에 따라 vApp의 스토리지 임대가 만료되기 전.	vApp의 소유자가 알림을 받거나 소유자가 시스템 관리자 인 경우 조직 관리자 가 알림을 받습니다.
VAPPTEMPLATE_STORAGE_NOTIFICATION_FAILED	vApp 템플릿 스토리지 임대 매트로가 임박했을 때 경고합니다. 임대 매트로가 만료되면 VMware Cloud Director가 vApp 템플릿을 삭제합니다.	구성된 배포 및 스토리지 임대 경고 시간에 따라 vApp 템플릿의 스토리지 임대가 만료되기 전.	vApp 템플릿의 소유자가 알림을 받거나 소유자가 시스템 관리자 인 경우 조직 관리자 가 알림을 받습니다.
VAPPTEMPLATE_STORAGE_NOTIFICATION_EXPIRED	vApp 템플릿 스토리지 임대 매트로가 임박했을 때 경고합니다. 임대 매트로가 만료되면 VMware Cloud Director가 vApp 템플릿을 만료된 것으로 표시합니다.	구성된 배포 및 스토리지 임대 경고 시간에 따라 vApp 템플릿의 스토리지 임대가 만료되기 전.	vApp 템플릿의 소유자가 알림을 받거나 소유자가 시스템 관리자 인 경우 조직 관리자 가 알림을 받습니다.
DISK_STORAGE_ALERT	디스크 스토리지 경고(빨간색 경고)	데이터스토어의 디스크 공간이 부족하고 빨간색 임계값에 도달했을 때.	시스템 관리자
DISK_STORAGE_ALERT_VDCS	제공자 VDC에 대한 디스크 스토리지 경고입니다. e-메일에는 하드 디스크 공간 부족으로 인해 빨간색 경고가 발생한 데이터스토어를 사용하는 제공자 VDC 목록이 포함되어 있습니다.	데이터스토어의 디스크 공간이 부족하고 빨간색 임계값에 도달했을 때.	시스템 관리자
VM_HW_UPGRADE_INVALID_POWERSTATE	VM의 전원 상태에 대한 알림입니다. 가상 하드웨어를 업그레이드하려면 VM의 전원을 켜야 합니다.	사용자가 VM의 하드웨어 버전을 업그레이드하려고 시도할 때.	VM의 소유자가 알림을 받거나 소유자가 시스템 관리자 인 경우 조직 관리자 가 알림을 받습니다.
VM_UPDATE_NESTED_HV_INVALID_POWERSTATE	VM의 전원 상태에 대한 알림입니다. 가상 하드웨어를 업그레이드하려면 VM의 전원을 켜야 합니다.	사용자가 VM의 하드웨어 버전을 업그레이드하려고 시도할 때.	VM의 소유자가 알림을 받거나 소유자가 시스템 관리자 인 경우 조직 관리자 가 알림을 받습니다.
FEDERATION_CERTIFICATE_SUCCESS	이벤트 인증서의 만료가 임박했을 때 모든 조직 관리자에게 페더레이션 인증서 만료 알림이 전송됩니다. 이 알림은 조직 관리자에게 SSO 서버에서 새 인증서를 다운로드하고 VMware Cloud Director를 업데이트하라는 메시지를 표시합니다.	페더레이션 인증서가 현재 날짜를 기준으로 7일 이내에 만료되는 경우.	조직 관리자
IPSEC_VPN_TUNNEL_ERROR	VPN 터널 오류(빨간색 경고)	VPN 터널이 작동하지 않을 때.	시스템 관리자
IPSEC_VPN_TUNNEL_ERROR_SUMMARY	VPN 터널 오류(빨간색 경고)	VPN 터널이 작동하지 않을 때.	시스템 관리자

표 5-22. VMware Cloud Director e-메일 알림 이름 (계속)

이름	설명	e-메일 전송 시점	받는 사람
IPSEC_VPN_TUNNEL_ENABLED	VPN 터널 사용(녹색 경고)	VPN 터널이 작동하지 않았다가 다시 작동할 때.	시스템 관리자
IPSEC_VPN_TUNNEL_ENABLED _SUMMARY			

표 5-23. 사용자 지정할 수 없는 e-메일 템플릿

알림	e-메일 전송 시점	받는 사람
vCenter Server 다시 연결됨 e-메일 경고	vCenter Server가 다시 연결되었을 때.	시스템 관리자
vCenter Server 연결 끊어짐 e-메일 경고. 이 e-메일에는 vCenter Server 연결 끊어짐의 원인이 오류 또는 사용자 요청인지 여부가 설명되어 있습니다.	vCenter Server의 연결이 끊어졌을 때.	시스템 관리자
AMQP 연결 끊어짐 e-메일 경고. AMQP 서버에서 VMware Cloud Director 연결이 끊어졌음을 알리는 경고입니다.	RabbitMQ가 작동을 중지할 때.	시스템 관리자
데이터베이스 연결 끊어짐 e-메일 경고	데이터베이스에서 VMware Cloud Director 연결이 끊어졌을 때.	시스템 관리자
데이터베이스 연결 복원됨 e-메일 경고	VMware Cloud Director가 데이터베이스에 다시 연결되었을 때.	시스템 관리자
스위치에서 호스트 연결 끊어짐 e-메일 경고	호스트가 사용 가능한 스위치에서 연결이 끊어졌을 때.	시스템 관리자
분산 가상 스위치에서 호스트 연결 끊어짐 e-메일 경고	호스트가 사용 가능한 분산 가상 스위치에서 연결이 끊어졌을 때.	시스템 관리자
LDAP 오류 e-메일 경고	LDAP와 동기화하는 동안.	시스템 관리자
LDAP 사용자 동기화 e-메일 경고	LDAP 사용자의 이름을 바꾸는 동안.	시스템 관리자
사이트 연결 상태 변경 e-메일 경고	최근에 사이트 연결이 끊어졌거나, 다시 연결되었거나, 여전히 다운된 상태입니다.	시스템 관리자

예제: e-메일 템플릿 업데이트

다음 명령은 DISK_STORAGE_ALERT_VDCS e-메일 템플릿의 현재 콘텐츠를 /tmp/DISK_STORAGE_ALERT_VDCS-new.txt라는 파일에서 생성한 콘텐츠로 바꿉니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#./cell-management-tool manage-email --set-template DISK_STORAGE_ALERT_VDCS /tmp/
DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s):
$pvdcList
"
Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from
```

```
$productName The $datastore is used by the followingProvider VDC(s): $pvdcsList
"

VCD Email notification details:
  name                : DISK_STORAGE_ALERT_VDCS
  description         : Alert when used disk storage exceeds threshold
  config key          : email.template.DISK_STORAGE_ALERT_VDCS.en-US
  template placeholders : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcsList]
  template content    : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcsList
```

연결이 끊어진 VM 찾기

셀 관리 도구의 `find-orphan-vms` 명령을 사용하여 vCenter 데이터베이스에는 있지만 VMware Cloud Director 데이터베이스에는 없는 가상 시스템에 대한 참조를 찾습니다.

vCenter 데이터베이스에서 참조되지만 VMware Cloud Director 데이터베이스에서는 참조되지 않는 가상 시스템은 연결이 끊어진 VM으로 간주됩니다. 이러한 가상 시스템에서 계산 리소스와 스토리지 리소스를 사용 중인 경우에도 VMware Cloud Director에서 이러한 가상 시스템에 액세스할 수 없기 때문입니다. 이러한 종류의 참조 불일치는 다량의 워크로드, 데이터베이스 오류, 관리 작업을 비롯한 여러 가지 이유로 발생할 수 있습니다. `find-orphan-vms` 명령을 사용하면 관리자가 이러한 VM을 나열한 후 제거하거나 VMware Cloud Director로 다시 가져올 수 있습니다. 이 명령에는 자체 서명된 인증서를 사용하는 VMware Cloud Director 또는 vCenter 설치 작업 시 필요할 수 있는, 대체 신뢰 저장소 지정을 위한 규정이 포함되어 있습니다.

다음 형식의 명령을 사용합니다.

```
cell-management-tool find-orphan-vms options
```

표 5-24. 셀 관리 도구 옵션과 인수, `find-orphan-vms` 하위 명령

옵션	인수	설명
<code>--help (-h)</code>	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--enableVerifyHostname</code>	없음	SSL 핸드셰이크의 호스트 이름 검증을 사용할 수 있도록 설정합니다.
<code>--host</code>	필수	연결이 끊어진 VM을 검색할 VMware Cloud Director 설치의 IP 주소 또는 정규화된 도메인 이름입니다.
<code>--output-file</code>	경로 이름 또는 -	연결이 끊어진 VM 목록이 기록되어야 할 파일의 전체 경로 이름입니다. 표준 출력에 목록을 기록하려면 -의 경로 이름을 지정합니다.
<code>--password (-p)</code>	필수	VMware Cloud Director 시스템 관리자 암호입니다.

표 5-24. 셀 관리 도구 옵션과 인수, find-orphan-vmns 하위 명령 (계속)

옵션	인수	설명
--port	VMware Cloud Director HTTPS 포트.	이 명령에서 기본 VMware Cloud Director HTTPS 포트를 사용하는 것을 원하지 않는 경우에만 이 옵션을 지정합니다.
--trustStore	Java 신뢰 저장소 파일에 대한 전체 경로 이름.	이 명령에서 기본 VMware Cloud Director 신뢰 저장소 파일을 사용하는 것을 원하지 않는 경우에만 이 옵션을 지정합니다.
--trustStorePassword	지정된 --trustStore 에 대한 암호	--trustStore 를 사용하여 대체 신뢰 저장소 파일을 지정하는 경우에만 필요합니다.
--trustStoreType	지정된 --trustStore (PKCS12, JCEKS, ...)의 유형	--trustStore 를 사용하여 대체 신뢰 저장소 파일을 지정하는 경우에만 필요합니다.
--user (-u)	필수	VMware Cloud Director 시스템 관리자 이름입니다.
--vc-name	필수	연결이 끊어진 VM을 검색할 vCenter의 이름입니다.
--vc-password	필수	vCenter 관리자 암호입니다.
--vc-user	필수	vCenter 관리자 이름입니다.

예제: 연결이 끊어진 VM 찾기

이 예제는 단일 vCenter Server를 쿼리합니다. --output-file 이 -로 지정되어 있기 때문에 결과가 표준 출력에 반환됩니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vmns \
--host 10.20.30.40 -u vcadmin -vc-name vcenter1 -vc-password P@55w0rd --vc-user admin --
output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc<->resource pool mappings associated with VC: 10.20.30.40 (https://
10.20.30.40:443)
Querying all vdc<->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...)
[moref: "resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test
```

```
VMs", parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test
VMs", parent moref : "group-v30533")
```

VMware 고객 환경 향상 프로그램 참여 또는 탈퇴

VMware CEIP(고객 환경 향상 프로그램)에 참여하거나 탈퇴하려면 셀 관리 도구의 `configure-ceip` 하위 명령을 사용하면 됩니다.

이 제품은 VMware CEIP(고객 환경 향상 프로그램)에 참여합니다. CEIP를 통해 수집된 데이터에 대한 세부 정보 및 VMware에서 이러한 정보를 사용하는 목적은 Trust & Assurance Center(<http://www.vmware.com/trustvmware/ceip.html>)에 명시되어 있습니다. 셀 관리 도구를 사용하여 언제라도 이 제품에 대해 VMware의 CEIP에 참여하거나 탈퇴할 수 있습니다.

```
cell-management-tool
configure-ceip
options
```

이 제품과 관련하여 VMware의 CEIP에 참여하지 않으려면 `--disable` 옵션과 함께 이 명령을 실행합니다.

표 5-25. 셀 관리 도구 옵션과 인수, `configure-ceip` 하위 명령

옵션	인수	설명
<code>--help</code> (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--disable</code>	없음	VMware 고객 환경 향상 프로그램을 탈퇴합니다.
<code>--enable</code>	없음	VMware 고객 환경 향상 프로그램에 참여합니다.
<code>--status</code>	없음	VMware 고객 환경 향상 프로그램에 대한 현재 참여 상태를 표시합니다.

예제: VMware 고객 환경 향상 프로그램 탈퇴

VMware 고객 환경 향상 프로그램에서 탈퇴하려면 다음과 같은 명령을 사용합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool configure-ceip --disableParticipation disabled
```

이 명령을 실행한 후에는 시스템에서 VMware 고객 환경 향상 프로그램에 더 이상 정보를 전송하지 않습니다.

VMware 고객 환경 항상 프로그램에 대한 현재 참여 상태를 확인하려면 다음과 같은 명령을 사용합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#cell-management-tool configure-ceip --statusParticipation disabled
```

애플리케이션 구성 설정 업데이트

셀 관리 도구의 manage-config 하위 명령으로 카탈로그 임계치 조절 작업과 같은 다양한 애플리케이션 구성 설정을 업데이트할 수 있습니다.

표 5-26. 셀 관리 도구 옵션과 인수, manage-config 하위 명령

옵션	인수	설명
--help (-h)	없음	이 하위 명령에 사용할 수 있는 옵션에 대한 요약을 보여 줍니다.
--delete (-d)	없음	대상 구성 설정을 제거합니다.
--lookup (-l)	없음	대상 구성 설정의 값을 조회합니다.
--name (-n)	구성 설정 이름	대상 구성 설정의 이름입니다. -d, -l 및 -v 옵션에 필요합니다.
--value (-v)	구성 설정 값	대상 구성 설정에 대한 값을 추가하거나 업데이트합니다.

예를 들어, [카탈로그 동기화 임계치 조절](#) 구성에 manage-config 하위 명령을 사용할 수 있습니다.

카탈로그 동기화 임계치 조절 구성

다른 조직에 게시되거나 다른 조직에서 구독된 카탈로그 항목이 많은 경우 카탈로그 동기화 중에 시스템 오버로드를 피하려면 카탈로그 동기화 임계치 조절을 구성하면 됩니다. 셀 관리 도구의 manage-config 하위 명령을 사용하여 동시에 동기화할 수 있는 라이브러리 항목 수를 제한하는 방식으로 카탈로그 동기화 임계치 조절을 구성할 수 있습니다.

구독된 카탈로그에서 카탈로그 동기화가 시작되면 게시된 카탈로그는 먼저 vCenter Server 저장소에서 VMware Cloud Director 전송 서비스 스토리지로 라이브러리 항목을 다운로드한 다음 구독된 카탈로그에 대한 다운로드 링크를 생성합니다. 게시된 모든 카탈로그가 동시에 다운로드할 수 있는 라이브러리 항목 수를 제한할 수 있습니다. 구독된 모든 카탈로그가 동시에 동기화할 수 있는 라이브러리 항목 수를 제한할 수 있습니다. 구독된 단일 카탈로그가 동시에 동기화할 수 있는 라이브러리 항목 수를 제한할 수 있습니다.

셀 관리 도구의 manage-config 하위 명령을 사용하여 카탈로그 임계치 조절에 대한 구성 설정을 업데이트할 수 있습니다. manage-config 하위 명령 사용에 대한 자세한 내용은 [애플리케이션 구성 설정 업데이트](#) 항목을 참조하십시오.

표 5-27. 카탈로그 임계치 조절에 대한 구성 설정

구성 설정	기본값	설명
<code>vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit</code>	30	<p>VMware Cloud Director 인스턴스의 게시된 모든 카탈로그가 vCenter Server에서 VMware Cloud Director로 동시에 다운로드할 수 있는 라이브러리 항목 수의 제한입니다.</p> <p>VMware Cloud Director 인스턴스 전체에서 다운로드할 게시된 라이브러리 항목의 총 수가 이 제한보다 큰 경우에는 이 제한에 따라 라이브러리 항목이 여러 부분으로 나뉘어 순차적으로 다운로드됩니다.</p>
<code>vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit</code>	30	<p>VMware Cloud Director 인스턴스의 구독된 모든 카탈로그가 동시에 동기화할 수 있는 라이브러리 항목 수의 제한입니다.</p> <p>VMware Cloud Director 인스턴스 전체에서 동기화할 구독된 라이브러리 항목의 총 수가 이 제한보다 큰 경우에는 이 제한에 따라 항목이 여러 부분으로 나뉘어 순차적으로 동기화됩니다.</p>
<code>contentLibrary.item.sync.batch.size</code>	10	<p>구독된 단일 카탈로그가 동시에 동기화할 수 있는 라이브러리 항목 수의 제한입니다.</p> <p>구독된 카탈로그가 이 제한보다 많은 라이브러리 항목 수를 동기화하려고 하면 이 제한에 따라 항목이 여러 부분으로 나뉘어 순차적으로 동기화됩니다.</p>

예제: 구독된 카탈로그에 대한 동기화 임계치 조절 구성

다음 명령은 구독된 단일 카탈로그가 동시에 동기화할 수 있는 라이브러리 항목 수 제한을 5로 설정합니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]# ./cell-management-tool manage-config -n contentLibrary.item.sync.batch.size -v 5
```

구독된 카탈로그에 라이브러리 항목이 13개 포함되어 있으면 카탈로그 동기화가 세 부분으로 나뉘어 순차적으로 수행됩니다. 첫 번째 부분은 다섯 개 항목을 포함하고 두 번째 부분은 그 다음 다섯 개 항목을 포함하고 마지막 부분은 나머지 세 개 항목을 포함합니다.

VMware Cloud Director 사용자 인터페이스에 대한 액세스 실패 문제 해결

VMware Cloud Director 환경에서 VMware Cloud Director 셀의 유효한 IP 주소와 DNS 항목을 살펴보고 업데이트하려면 셀 관리 도구의 `manage-config` 하위 명령을 사용하면 됩니다.

문제

로그인에 성공한 후 VMware Cloud Director Service Provider Admin Portal이나 VMware Cloud Director Tenant Portal에 액세스할 수 없습니다.

로그인 화면에 자격 증명을 입력하면 다음 오류 메시지가 표시됩니다. 시작하지 못했습니다. 초기화하는 동안 오류가 발생했습니다. 이 문제는 지원되지 않는 공용 URL을 통한 애플리케이션 액세스 또는 연결 불량과 같은 문제로 인해 발생할 수 있습니다.

원인

VMware Cloud Director는 CORS(원본 간 리소스 공유) 필터 구현을 사용하여 Service Provider Admin Portal 및 VMware Cloud Director Tenant Portal에 액세스하는 데 사용할 수 있는 모든 유효한 끝점 목록을 유지 관리합니다.

CORS 필터링 목록은 셀 구성 중에 채워지고 업데이트됩니다. 여기에는 서버 그룹의 모든 셀에 대한 IP 주소 및 DNS 이름을 포함하는 HTTP 및 HTTPS 항목이 포함됩니다. 또한 VMware Cloud Director 서버 그룹을 향하는 로드 밸런서에 사용되는 공개 IP 주소도 포함됩니다.

장치 배포의 셀 구성 중에 목록이 VMware Cloud Director 셀의 DNS 이름으로 업데이트되지 않으며 셀의 DNS 이름을 사용하여 액세스할 수 없습니다.

해결책

- 1 서버 그룹의 셀 중 하나에 **루트**로 로그인하거나 SSH를 실행합니다.
- 2 환경에서 VMware Cloud Director 셀에 액세스하는 데 사용할 수 있는 유효한 URL을 나열하려면 다음 명령줄을 실행합니다.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n webapp.allowed.origins -l
```

시스템 출력은 서버 그룹의 모든 셀에 대한 IP 주소 및 DNS 이름이 있는 HTTP 및 HTTPS 항목을 포함하는 목록입니다. 또한 VMware Cloud Director 서버 그룹을 향하는 로드 밸런서에 사용되는 공개 IP 주소도 포함됩니다.

이 목록은 항목 사이에 공백 없이 쉼표로 구분된 문자열입니다.

- 3 (선택 사항) webapp.allowed.origins 구성 설정을 업데이트하려면 다음 명령줄을 실행합니다. 명령줄에서 설정의 값 매개 변수는 IP 주소 및 DNS 이름 목록이며, 항목 사이에 공백 없이 쉼표로 구분된 문자열입니다.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n webapp.allowed.origins -v "comma_separated_list_of_URLs_without_spaces"
```

vCenter VM 검색 디버깅

셀 관리 도구의 debug-auto-import 하위 명령을 사용하면 vApp을 검색하는 메커니즘이 하나 이상의 vCenter VM을 건너뛰는 이유를 조사할 수 있습니다.

기본 구성을 사용할 경우 조직 VDC는 해당 VDC를 지원하는 리소스 풀에 만들어진 vCenter VM을 자동으로 검색합니다. "VMware Cloud Director 서비스 제공자 관리자 포털 가이드"에서 vApp 정보 검색 및 채택을 참조하십시오. vCenter VM이 검색된 vApp에 표시되지 않으면 이 VM 또는 VDC에 대해 debug-auto-import 하위 명령을 실행할 수 있습니다.

```
cell-management-tool debug-auto-import options
```

debug-auto-import 하위 명령은 검색 메커니즘에서 건너편 vCenter VM 목록 및 가능한 이유에 대한 정보를 반환합니다. 이 목록에는 검색되었지만 조직 VDC로 가져오지 못한 vCenter VM도 포함됩니다.

표 5-28. 셀 관리 도구 옵션과 인수, debug-auto-import 하위 명령

옵션	인수	설명
--help (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
--org	조직 이름	선택 사항입니다. 지정된 조직에 대해 건너편 VM에 대한 정보를 나열합니다.
--vm	VM 이름 또는 VM 이름의 일부	지정된 VM 이름을 포함하는 건너편 VM에 대한 정보를 나열합니다. --org 옵션을 사용할 경우 선택 사항입니다.

예제: VM 이름 test로 vCenter VM 검색 디버그

다음 명령은 모든 조직에서 건너편 vCenter VM에 대한 정보를 반환합니다.

```
[root@cell11 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc  
can be skipped for the following reasons:
```

- 1) Virtual machine is already imported in vCD or is managed by vCD
- 2) Virtual machine is created by vCD

```
VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc  
can be skipped for the following reasons:
```

- 1) Virtual machine is not present in a vCD managed resource pool

```
VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
```

- 1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry

이 예에서 시스템 출력은 검색 메커니즘에서 건너뛰고 이름에 문자열 test가 포함된 세 개의 vCenter VM에 대한 정보를 반환합니다. VM import-test3은 검색되었지만 VDC로 가져오지 못한 VM의 예입니다.

다중 사이트에 스트레치된 네트워크에 대한 MAC 주소 재생성

동일한 설치 ID로 구성된 두 개의 VMware Cloud Director 사이트를 연결하는 경우에는 사이트 전반에 스트레치된 네트워크에서 MAC 주소 충돌이 발생할 수 있습니다. 이러한 충돌을 피하려면 설치 ID와는 다른 사용자 지정 시드를 기반으로 사이트 중 하나에서 MAC 주소를 재생성해야 합니다.

초기 VMware Cloud Director 설정 중에 설치 ID를 설정합니다. VMware Cloud Director는 설치 ID를 사용하여 가상 시스템 네트워크 인터페이스에 대한 MAC 주소를 생성합니다. 동일한 설치 ID로 구성된 두 개의 VMware Cloud Director 설치에는 동일한 MAC 주소를 생성할 수 있습니다. MAC 주소가 중복되면 연결된 두 사이트 간에 스트레치된 네트워크에서 충돌이 발생할 수 있습니다.

동일한 설치 ID로 구성되고 연결된 사이트 간에 스트레치된 네트워크를 생성하기 전에 셀 관리 도구의 `mac-address-management` 하위 명령을 사용하여 두 사이트 중 하나에서 MAC 주소를 재생성해야 합니다.

```
cell-management-tool mac-address-management options
```

새 MAC 주소를 생성하려면 설치 ID와는 다른 사용자 지정 시드를 설정합니다. 시드는 설치 ID를 덮어쓰지 않습니다. 단, 데이터베이스가 최신 시드를 두 번째 구성 매개 변수로 저장하며, 이것이 설치 ID를 재정의합니다.

서버 그룹의 임의 VMware Cloud Director 구성원에서 `mac-address-management` 하위 명령을 실행합니다. 이 명령은 VMware Cloud Director 데이터베이스에 대해 실행되므로 서버 그룹에 대해 명령을 한 번만 실행합니다.

중요 MAC 주소를 재생성하려면 VMware Cloud Director의 다운타임이 필요합니다. 재생성을 시작하기 전에 서버 그룹의 모든 셀에서 작업을 중지해야 합니다.

표 5-29. 셀 관리 도구 옵션과 인수, `mac-address-management` 하위 명령

옵션	인수	설명
<code>--help</code> (-h)	없음	이 범주에서 사용할 수 있는 명령에 대한 요약을 보여 줍니다.
<code>--regenerate</code>	없음	사용하지 않는 MAC 주소를 모두 삭제하고 현재 시드를 기반으로 새 MAC 주소를 생성합니다. 이전에 설정한 시드가 없으면 설치 ID를 기반으로 MAC 주소가 재생성됩니다. 사용 중인 MAC 주소는 보존됩니다.

참고 서버 그룹의 모든 셀은 비활성 상태여야 합니다. 셀에서 작업을 중지하는 방법에 대한 자세한 내용은 [셀 관리](#) 항목을 참조하세요.

표 5-29. 셀 관리 도구 옵션과 인수, mac-address-management 하위 명령 (계속)

옵션	인수	설명
--regenerate-with-seed	0~63 사이의 시드 번호	데이터베이스에 새 사용자 지정 시드를 설정하고 사용 중이 아닌 MAC 주소를 모두 삭제하고 새로 설정된 시드를 기반으로 새 MAC 주소를 생성합니다. 사용 중인 MAC 주소는 보존됩니다. 참고 서버 그룹의 모든 셀은 비활성 상태여야 합니다. 셀에서 작업을 중지하는 방법에 대한 자세한 내용은 셀 관리 항목을 참조하세요.
--show-seed	없음	현재 시드 및 각 시드에 사용 중인 MAC 주소 수를 반환합니다.

중요 사용 중인 MAC 주소는 보존됩니다. 사용 중인 MAC 주소를 재생성된 MAC 주소로 변경하려면 네트워크 인터페이스 MAC 주소를 재설정해야 합니다. 가상 시스템 속성을 편집하는 방법에 대한 자세한 내용은 "VMware Cloud Director 테넌트 포털 가이드" 항목을 참조하십시오.

예제: 새 사용자 지정 시드를 기반으로 MAC 주소 재생성

다음 명령은 현재 시드를 9로 설정하고 새로 설정된 시드를 기반으로 사용 중이 아닌 모든 MAC 주소를 재생성합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#./cell-management-tool mac-address-management --regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses.
Successfully generated new MAC addresses.
```

예제: 현재 시드 및 각 시드에 사용 중인 MAC 주소 수 보기

다음 명령은 현재 시드 및 시드당 MAC 주소 수에 대한 정보를 반환합니다.

```
[root@cell11 /opt/vmware/vcloud-director/
bin]#./cell-management-tool mac-address-management --show-seed
Current MAC address seed is '9' and based on MacAddressSeed config.
MAC address seed    9 is in use by      12 MAC addresses
MAC address seed    1 is in use by      1 MAC addresses
```

이 예에서는 시스템 출력에 현재 시드가 9이고 이 시드를 기반으로 하는 12 개의 MAC 주소가 있는 것이 표시됩니다. 또한 이전 시드 또는 설치 ID 1을 기반으로 하는 MAC 주소가 하나 있습니다.

VMware Cloud Director 셀의 데이터베이스 IP 주소 업데이트

데이터베이스 고가용성 클러스터에서 VMware Cloud Director 셀의 IP 주소를 업데이트하려면 셀 관리 도구를 사용하면 됩니다.

사전 요구 사항

데이터베이스 고가용성 클러스터에서 셀의 IP 주소를 업데이트하려면 현재 기본 노드의 IP 주소를 제공해야 합니다. IP 주소를 찾으려면 VMware Cloud Director 장치 API를 사용하여 클러스터에 있는 대기 노드의 노드 ID를 기록해 둡니다. <http://code.vmware.com>에서 "VMware Cloud Director 장치 API 스키마 참조"의 내용을 참조하십시오.

절차

- 1 클러스터에 있는 셀의 OS에 **root**로 직접 로그인하거나 SSH 클라이언트를 사용하여 로그인합니다.
- 2 셀이 해당 노드에서 실행 중인지 확인합니다.

```
service vmware-vcd pid cell
```

셀 프로세스 ID가 NULL이 아니면 VMware Cloud Director 셀이 실행 중이며 VMware Cloud Director 셀을 다시 시작하지 않고 데이터베이스의 IP 주소를 변경할 수 있습니다.

- 3 서버 그룹의 모든 셀에서 IP 주소를 업데이트하려면 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address --pid cell process ID --remote-sudo-user postgres --private-key-path /opt/vmware/vcloud-director/id_rsa
```

시스템 출력에 재구성이 완료된 것이 표시됩니다.

- 4 (선택 사항) 각 VMware Cloud Director 셀이 올바른 데이터베이스 IP 주소를 가리키고 있는지 확인합니다.

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

시스템 출력에 셀이 업데이트된 것이 표시됩니다.

- 5 셀 중 하나라도 업데이트되지 않으면 명령을 실행하여 다시 구성합니다.

- 셀이 실행되고 있지 않으면 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address
```

- 셀이 실행 중이면 다음 명령을 실행합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address -i cell process ID
```

6 실행되고 있지 않은 셀을 재구성한 경우, 명령을 실행하여 `vmware-vcd`를 다시 시작합니다.

a 다음 명령을 실행하여 서비스를 중지합니다.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid cell) -s
```

b 다음 명령을 실행하여 서비스를 시작합니다.

```
systemctl start vmware-vcd
```

VMware Cloud Director 로그 수집

6

VMware Cloud Director는 서버 그룹의 각 클라우드 셀에 대한 로깅 정보를 제공합니다. 로그를 확인하여 셀을 모니터링하고 VMware Cloud Director를 실행하는 동안 발생하는 문제를 해결할 수 있습니다.

VMware Cloud Director 로그

로그 이름 파일 또는 디렉토리	설명
/opt/vmware/vcloud-director/logs/cell.log	VMware Cloud Director 셀의 콘솔 출력입니다.
/opt/vmware/vcloud-director/logs/cell-management-tool	셀에서 생성된 셀 관리 도구 로그 메시지입니다.
/opt/vmware/vcloud-director/logs/cell-runtime	셀에서 생성된 런타임 로그 메시지입니다.
/opt/vmware/vcloud-director/logs/cloud-proxy	셀에서 생성된 클라우드 프록시 로그 메시지입니다.
/opt/vmware/vcloud-director/logs/console-proxy	셀에서 생성된 원격 콘솔 프록시 로그 메시지입니다.
/opt/vmware/vcloud-director/logs/server-group-communications	셀에서 생성된 서버 그룹 통신입니다.
/opt/vmware/vcloud-director/logs/statsfeeder	vCenter Server의 가상 시스템 메트릭 검색 및 스토리지 정보 및 오류 메시지입니다.
/opt/vmware/vcloud-director/logs/vcloud-container-debug.log	셀에서 생성된 디버그 수준 로그 메시지입니다.
/opt/vmware/vcloud-director/logs/vcloud-container-info.log	셀에서 생성된 정보 로그 메시지입니다. 이 로그는 셀에서 발생한 경고나 오류를 보여 줍니다.
/opt/vmware/vcloud-director/logs/vmware-vcd-watchdog.log	셀 감시에서 생성된 정보 로그 메시지입니다. 셀이 응답을 중지하고 다시 시작되는 경우 등을 기록합니다.
/opt/vmware/vcloud-director/logs/diagnostics.log	셀 진단 로그입니다. 로컬 로깅 구성에서 진단 로깅을 사용하도록 설정하지 않은 경우 이 파일은 비어 있습니다.
/opt/vmware/vcloud-director/logs/YYYY_MM_DD.request.log	Apache 일반 로그 형식의 HTTP 요청 로그입니다.

VMware Cloud Director 장치 로그

VMware Cloud Director 장치에는 몇 가지 추가 로그 파일이 있습니다.

로그 파일	설명
/opt/vmware/var/log/firstboot	장치의 첫 번째 부팅과 관련된 로깅 정보가 포함됩니다.
/opt/vmware/var/log/vcd	Replication Manager(repmgr) 도구 모음 설정, 재구성, 장치 동기화와 관련된 로그가 포함됩니다.
/opt/vmware/var/log/vcd/pg	내장된 장치 데이터베이스의 백업과 관련된 로그가 포함됩니다.
/opt/vmware/etc/vami/ovfEnv.xml	OVF 배포 매개 변수를 포함합니다.
/var/vmware/vpostgres/current/pgdata/log	내장형 PostgreSQL 데이터베이스와 관련된 로그가 포함됩니다.
/opt/vmware/var/log/vami/updatecli.log	장치 업그레이드와 관련된 로깅이 포함됩니다.

텍스트 편집기, 텍스트 뷰어 또는 타사 도구를 사용하여 로그를 볼 수 있습니다.

VMware Cloud Director 소프트웨어 제거

7

Linux rpm 명령을 사용하여 개별 서버에서 VMware Cloud Director 소프트웨어를 제거할 수 있습니다.

절차

- 1 대상 서버에 **root**로 로그인합니다.
- 2 일반적으로 /opt/vmware/vcloud-director/data/transfer에 마운트되어 있는 전송 서비스 스토리지를 마운트 해제합니다.
- 3 콘솔, 셸 또는 터미널 창을 열고 Linux rpm 명령을 실행합니다.

```
rpm -e vmware-phonehome vmware-vcloud-director vmware-vcloud-director-rhel
```

설치된 다른 패키지가 vmware-vcloud-director 패키지에 종속된 경우, VMware Cloud Director를 제거하기 전에 해당 패키지를 제거하라는 메시지가 표시됩니다.